HEALTH AFFAIRS

TRICARE
Management
Activity

Protected Health Information Management Tool (PHIMT)

Quarterly Training

February 2005

TMA Privacy Office

Agenda

- Overview of PHIMT
- PHIMT User Interface
- User Admin Functionality
- Privacy Specialist/Regular User Functionality
- Administrative Summary

Training Objectives

- Once you have completed this course, you will be able to:
  - Describe the PHIMT application
  - Identify the user roles and permissions
  - Perform the functions of the User Admin, Privacy Specialist, and Regular User within the PHIMT

PHIMT Overview

Objectives

- Upon completion of this lesson, you will be familiar with the:
  - Commercial Off The Shelf (COTS) product customization
  - PHIMT Terminology
  - User roles and associated permissions
  - Hierarchy

Customized COTS Product

- COTS product built for HIPAA Privacy
- Browser-based
- Centrally administered
- Shared database
- Designed to perform fundamental tasks
  - Accounting of Disclosures
  - Record retrieval requirements
- Consolidation of multiple tasks into an electronic environment

Terminology

- **User** - an individual with a unique login ID and Password assigned to an organization within the tool

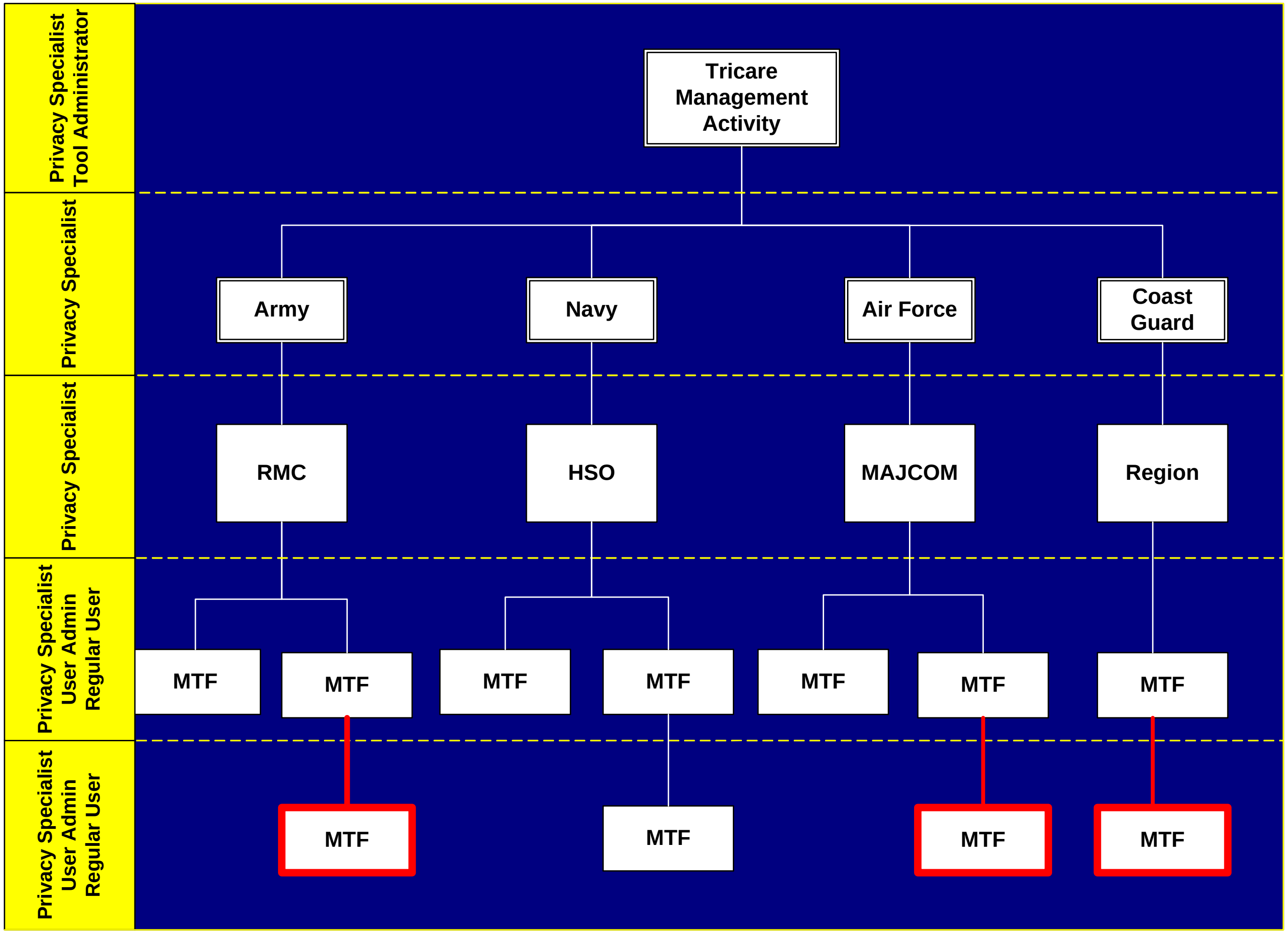
- **Organization** - a logical or physical entity such as an MTF, a Service or TRICARE Management Activity

- **Role** - a named collection of permissions within the tool
  A user can have the same roles in multiple organizations, or different roles in multiple organizations

User Roles and Permissions

- **User Admin** is a local admin for an MTF or a designated Service. This role allows one to add/modify users from within their Service and assign roles. This role will be handled by the email account administrators for each MTF or Service
- **Privacy Specialist** is the Privacy Officer or designee at an MTF or Service level. This role allows the user to maintain disclosure reporting, approve/deny disclosure requests, amendments to requests, restrictions to disclosures, disclosure suspensions and generate associated letters
- **Regular User** is a general role with basic functionality. This role can create disclosures and authorization requests that can be routed on to a Privacy Specialist

PHIMT Overview
Hierarchy



* These do not exist at this point, but can be added to the PHIMT

Summary

- You should now be familiar with the:
  - COTS product customization
  - PHIMT Terminology
  - User roles and associated permissions
  - Hierarchy

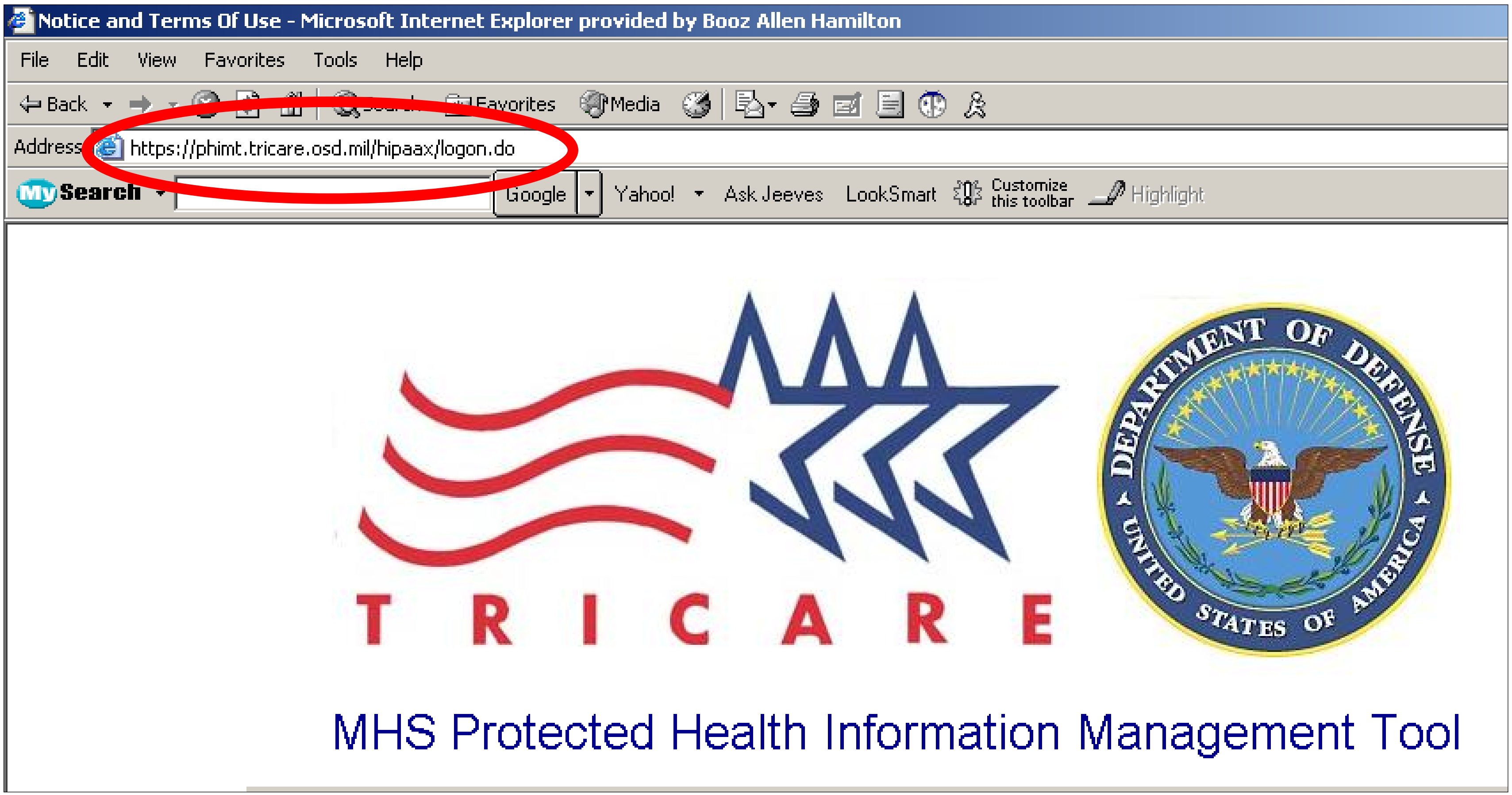
PHIMT User Interface

Objectives

- Upon completion of this lesson, you will be able to locate the:
  - Login Screen
  - Patient Tab
  - User Tab
  - Admin Tab
  - Requests Tab
  - Requester Tab

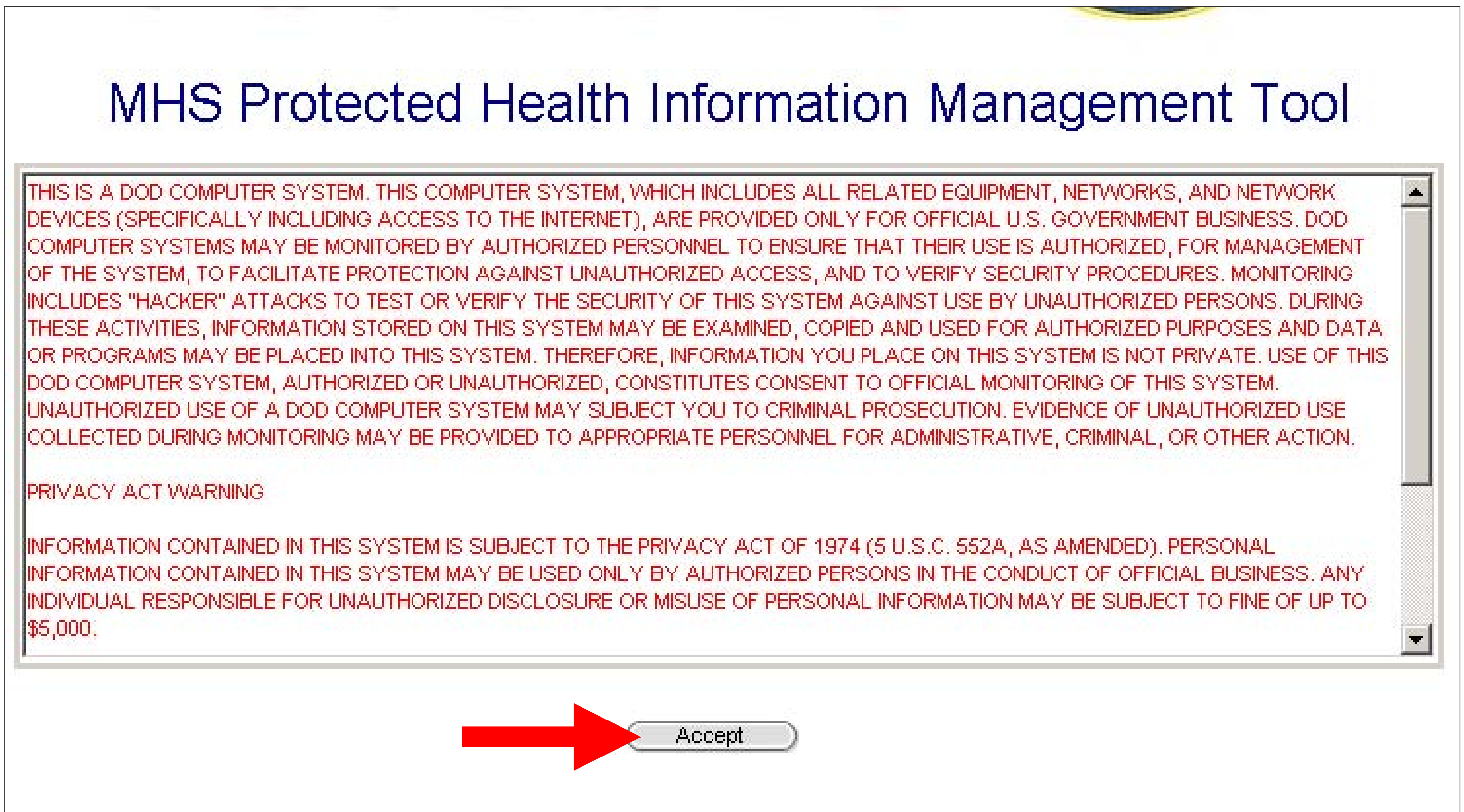
PHIMT User Interface
Login Screen

1. Enter the URL: https://phimt.tricare.osd.mil



PHIMT User Interface
Login Screen

2. Read the Notice and Terms of Use
3. Click on the Accept button

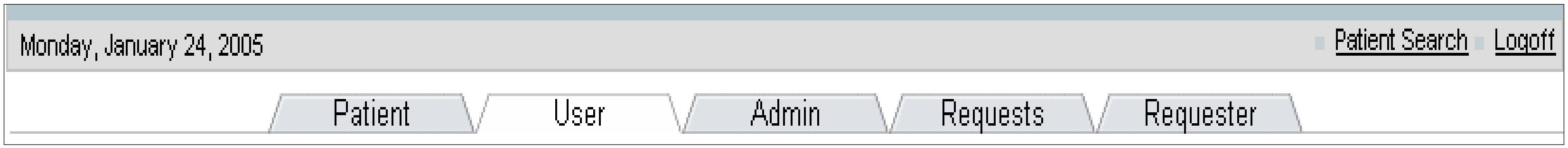


Login Screen

3. Type in User Name and Password
4. Click on the Login button

PHIMT User Interface

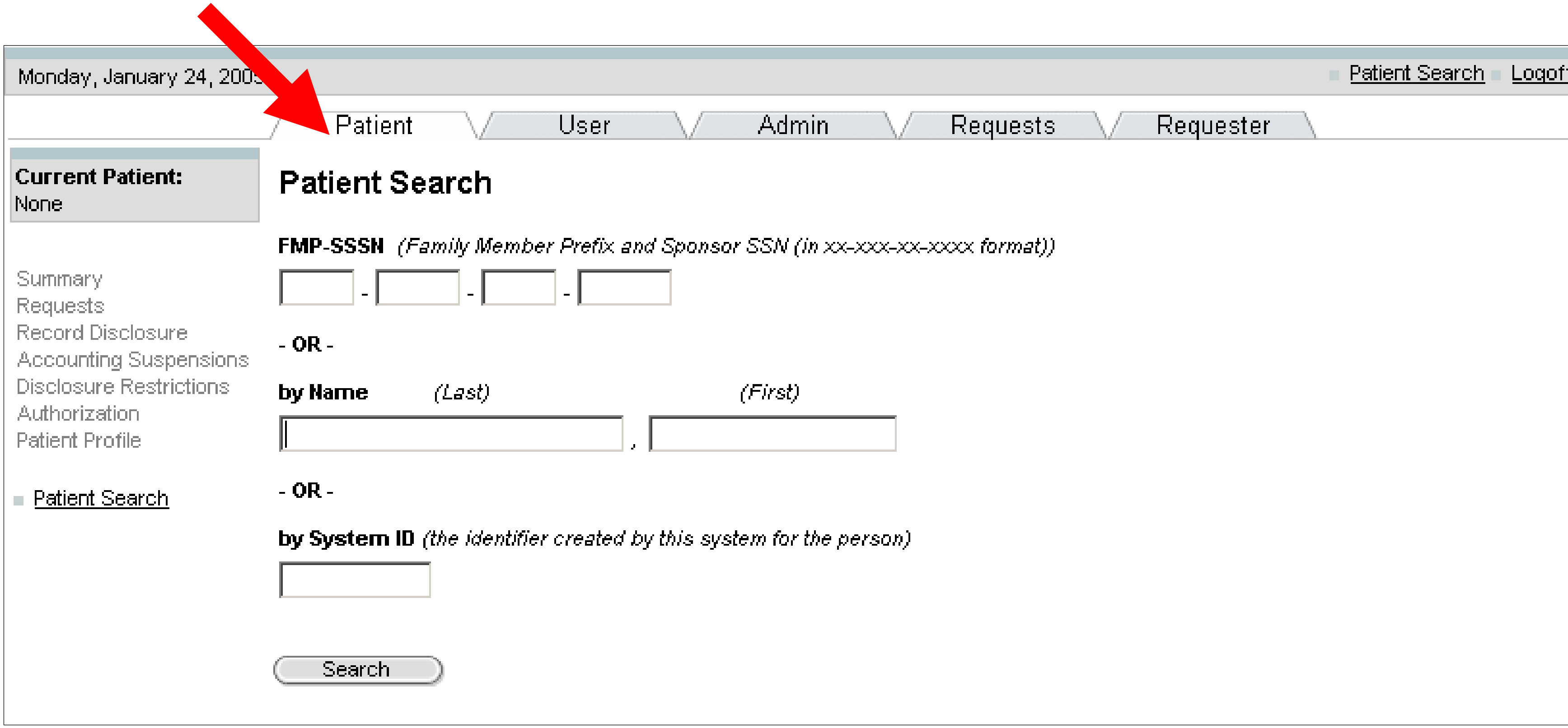
Tabs



- Patient
- User
- Admin
- Requests
- Requester

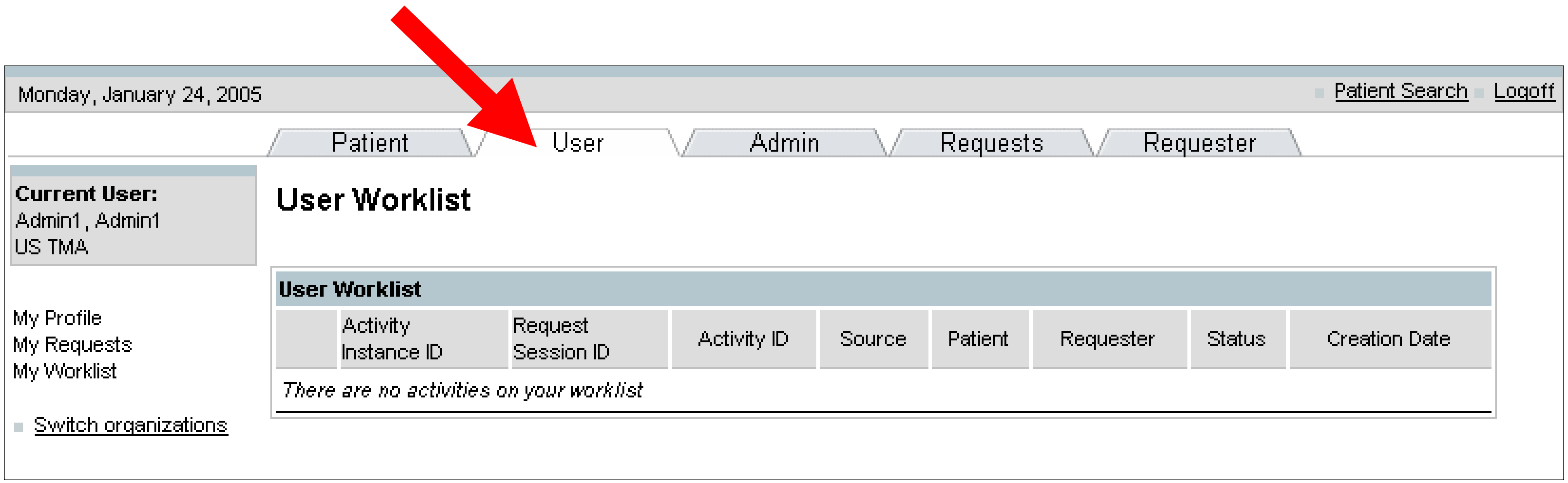
PHIMT User Interface

Patient Tab



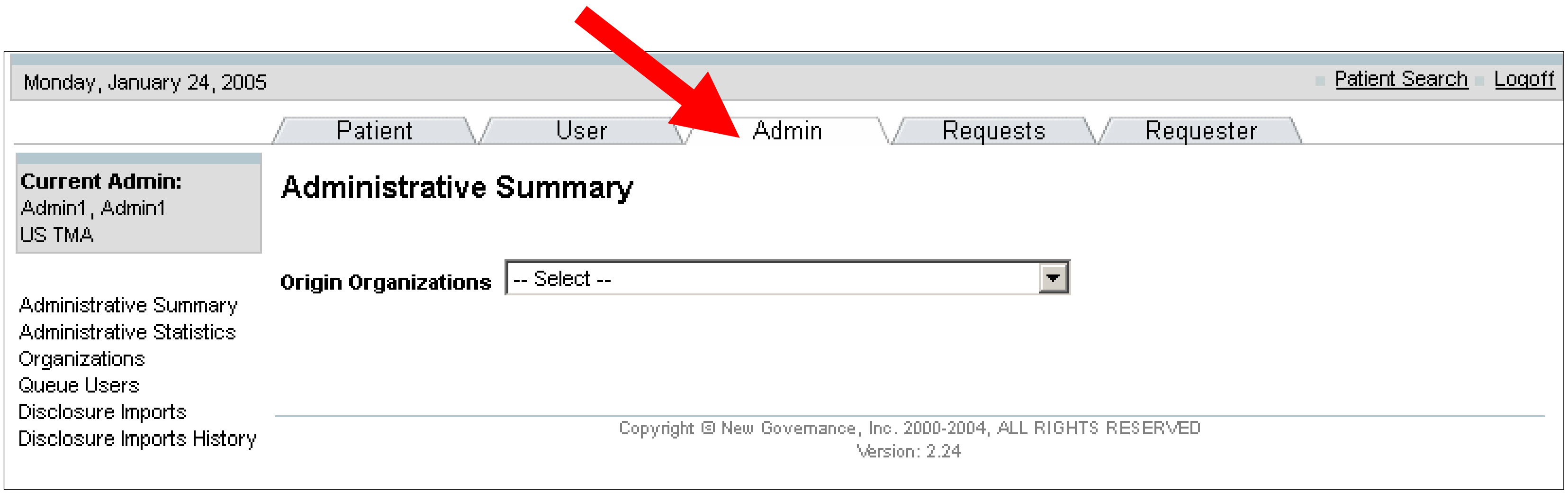
PHIMT User Interface

User Tab



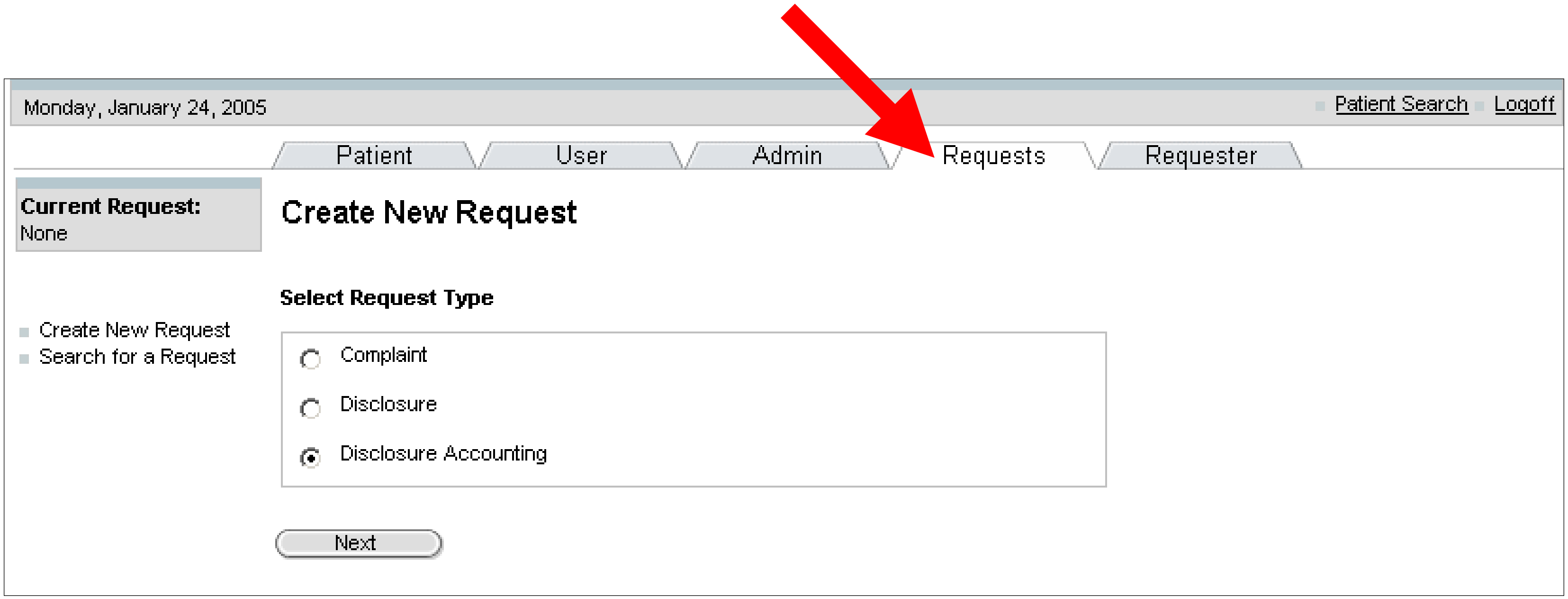
PHIMT User Interface

Admin Tab



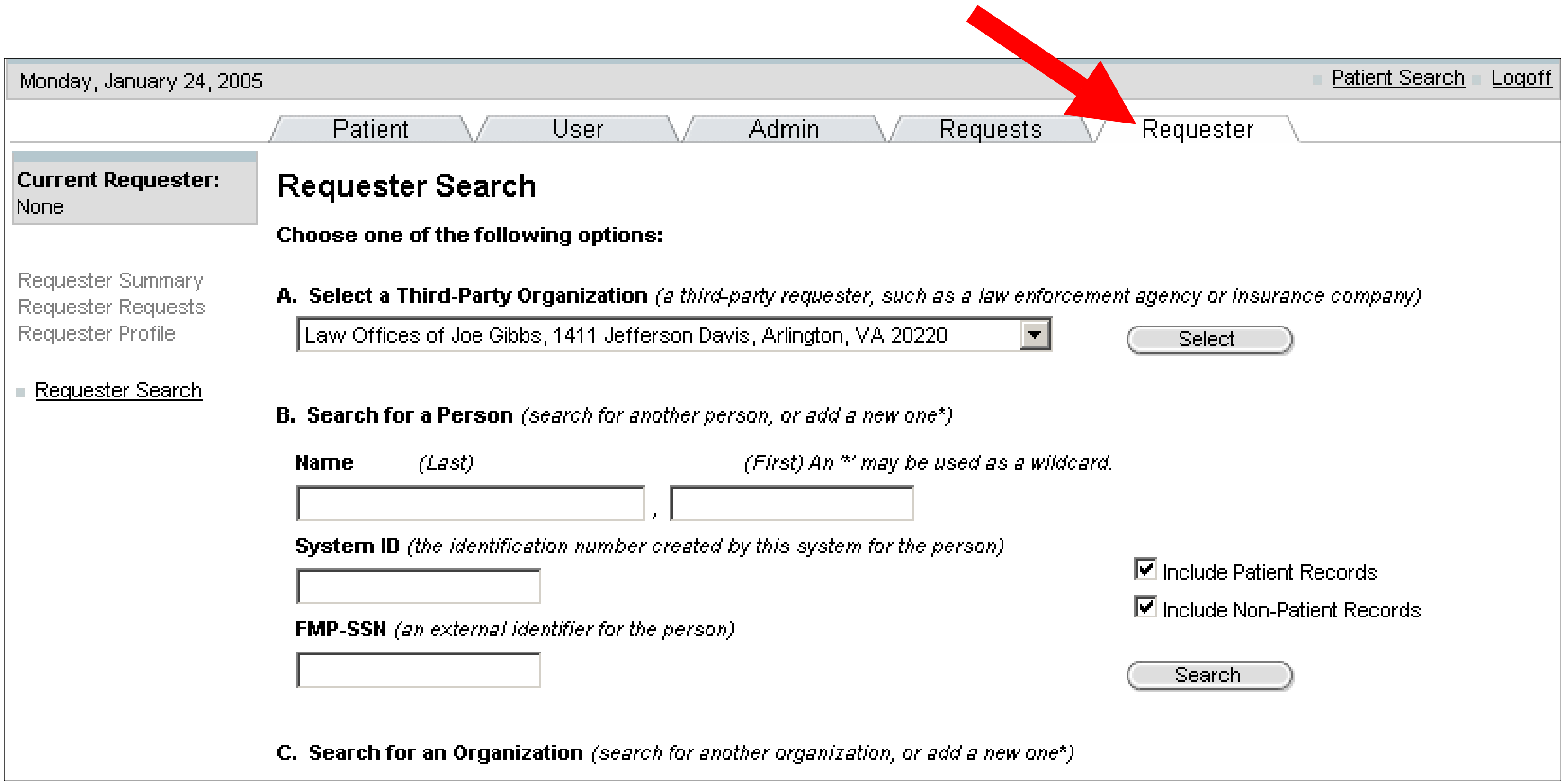
PHIMT User Interface

Requests Tab



PHIMT User Interface

Requester Tab



Summary

- You should now be able to locate the:
  - Login Screen
  - Patient Tab
  - User Tab
  - Admin Tab
  - Requests Tab
  - Requester Tab

User Admin Functionality

Objectives

- Upon completion of this lesson, you will be able to:
  - Describe the process of obtaining a User Admin account
  - Create user accounts
  - Setup a workflow
  - Setup a queue
  - Create requester favorites
  - Disable users
  - Transfer users

User Admin Functionality

Obtain a User Admin Account

- Requests for User Admins to be created must be routed to and approved by the Service Representative
- The Service Representative will route the approved request to the HIPAA Support Center
- The HIPAA Support Center will establish the User Admin account and provide the User Admin login information to the appropriate individual

User Admin Functionality

Create User Accounts

- The User Admin is responsible for adding users and assigning roles to the users within their organization

- User Admin provides the user with their login information

- Determined by Service specific requirements or MTF requirements

User ID and Password Requirements

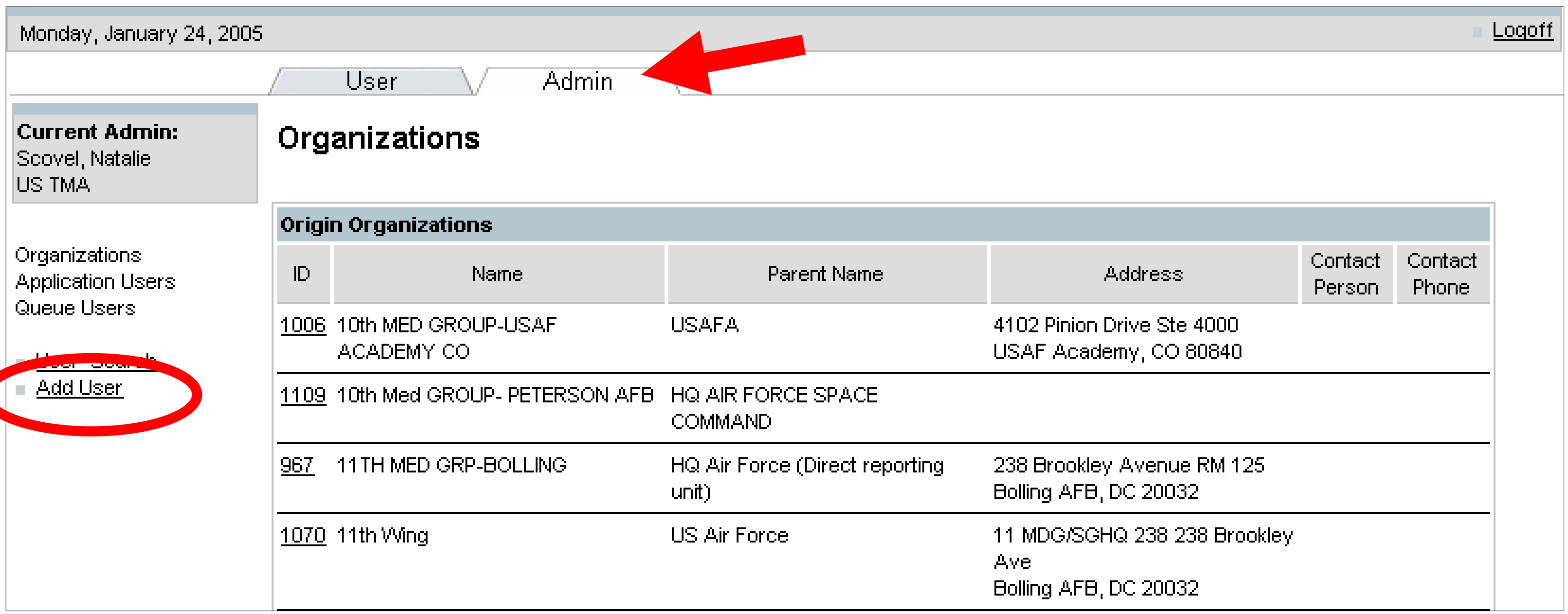
- User ID:
  - Assigned by the User Admin, usually first initial of the first name and complete last name (follow Service guidelines)
  - Duplicate User Name not allowed by the application

- Password:
  - 8-15 characters long and must contain at least one
  - Alphabetical uppercase character
  - Alphabetical lower case character
  - Arabic numeral (0, 1, 2, 3, 4)
  - Non-alphanumeric special character (I.e. !, @, #, $, etc.)

User Admin Functionality

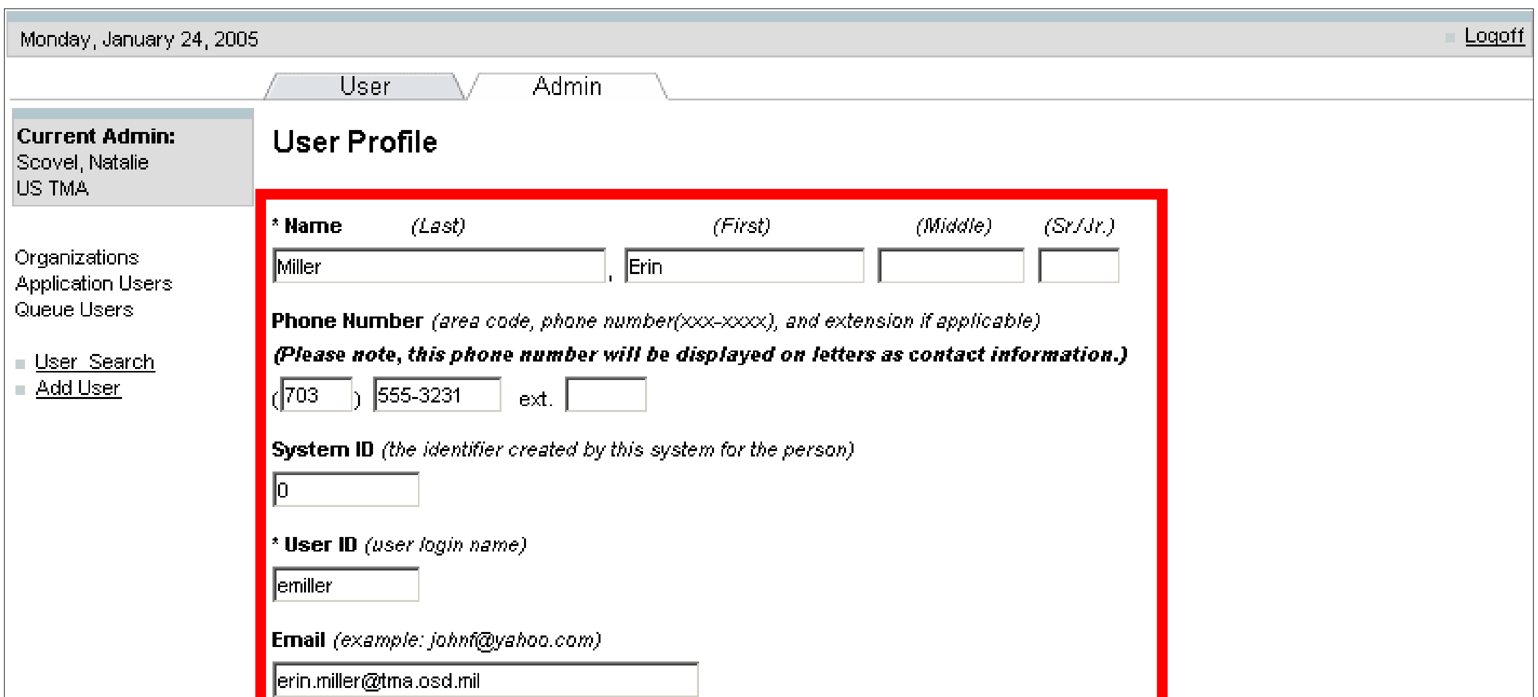
Create User Accounts (1 of 3)

1. Select the Admin Tab
2. Select the Add User hyperlink



Create User Accounts (2 of 3)

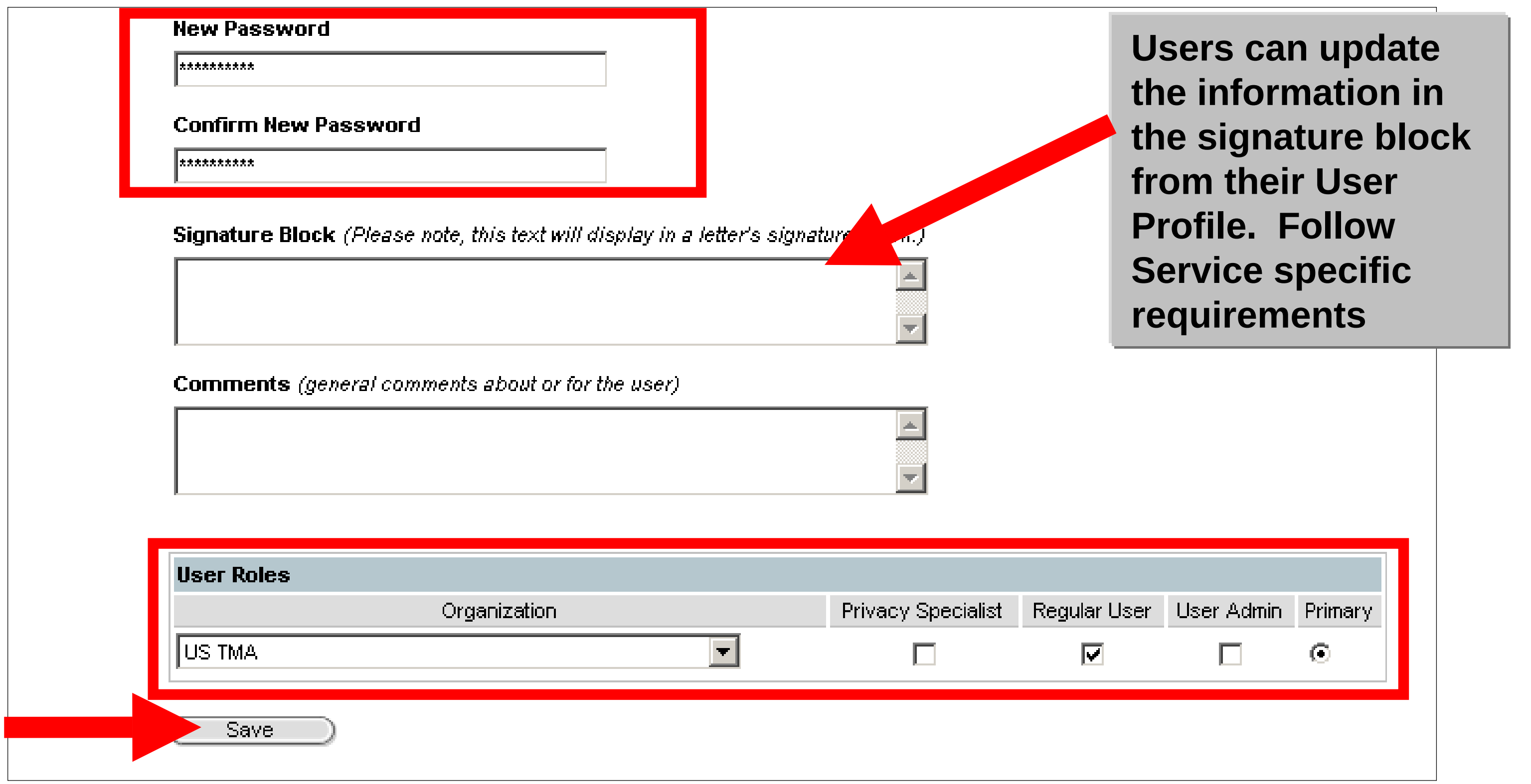
3. Enter user information (name, phone number and email address)
4. Enter a unique User ID (No duplicate IDs are allowed across all Services)



User Admin Functionality

Create User Accounts (3 of 3)

5. Enter a temporary new password and confirm new password
6. Select organization from the drop-down box and select the appropriate user role
7. Click on the Save button



User Admin Functionality

Workflow Setup (1 of 6)

- Once a user has been added and their organization and user role is established, the User Admin can establish the workflow for that user’s disclosures
- The workflow delineates the process by which requests are routed within the system
- Workflows should be set up so that a Regular Users work will be routed to a Privacy Specialist for approval or denial

User Admin Functionality

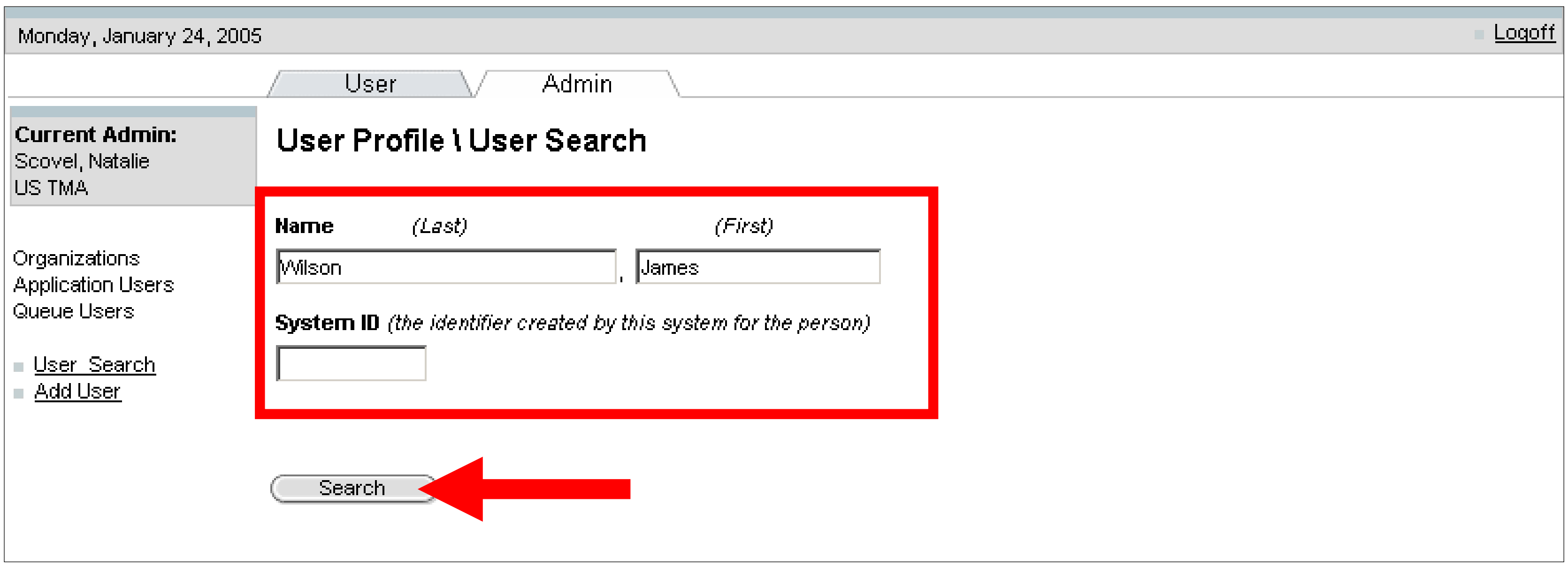
Workflow Setup (2 of 6)

1. Scroll to the bottom of the User Profile screen
2. Click on the New button next to Privacy Specialists

User Admin Functionality

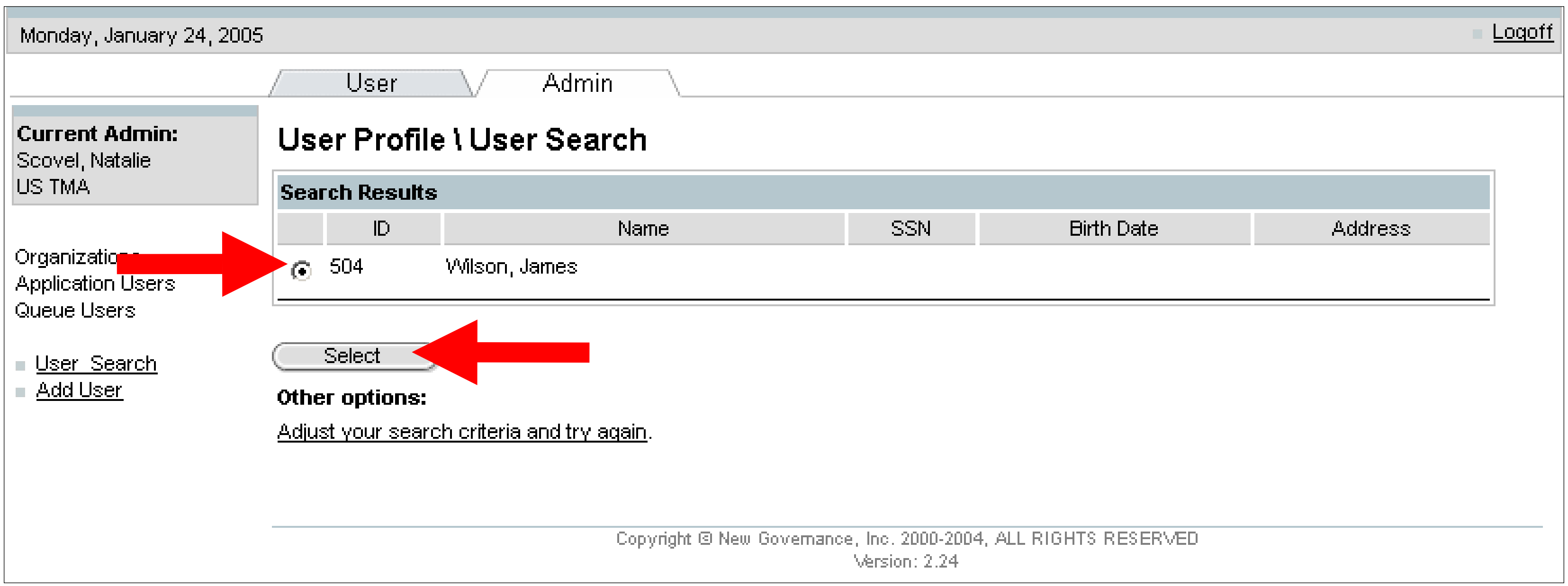
Workflow Setup (3 of 6)

3. Enter search criteria
4. Click on the Search button



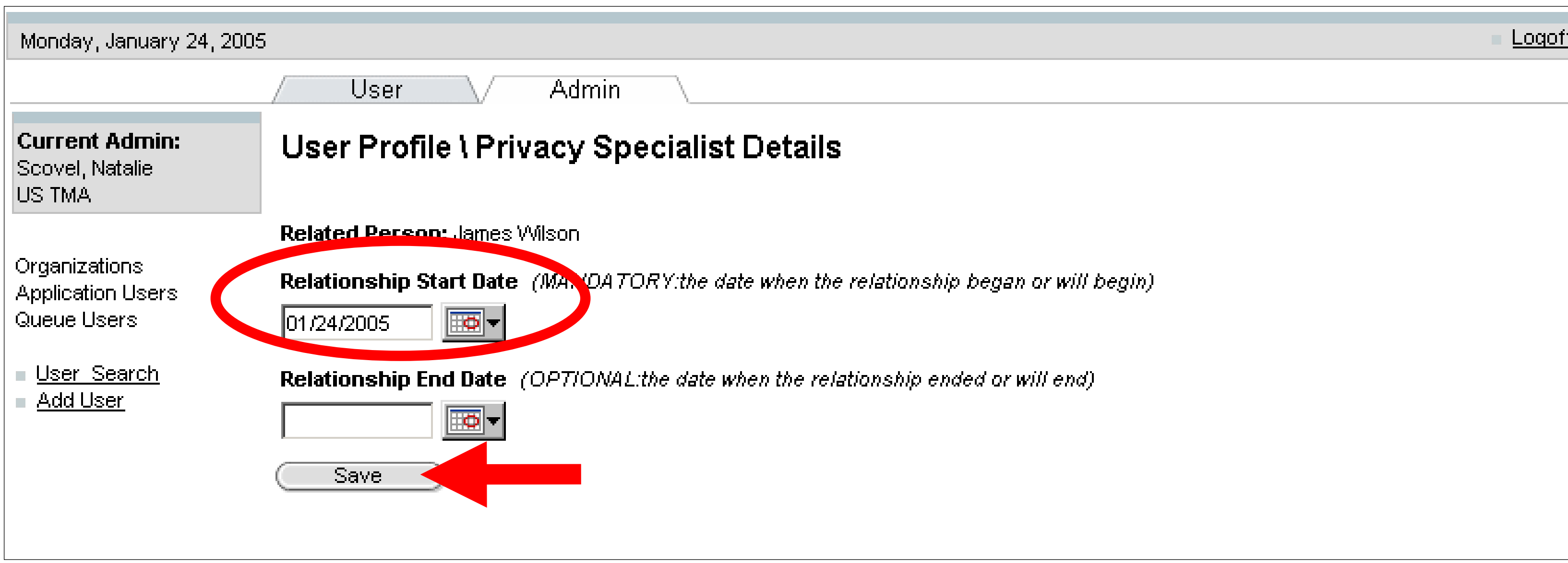
Workflow Setup (4 of 6)

5. Select the appropriate Privacy Specialist from the search results and click on the Select button



Workflow Setup (5 of 6)

6. Set Relationship Start Date / End Date (End Date optional)
7. Click on the Save button



Workflow Setup (6 of 6)

8. Privacy Specialist is added to the User Profile screen

Allowed Worklist Viewers New

Name	Start Date	End Date
There are no Allowed Worklist Viewers configured. Click new to add one.		

Backup Persons New

Name	Start Date	End Date
There are no Backup Persons configured. Click new to add one.		

Information Officers New

Name	Start Date	End Date
There are no Information Officers configured. Click new to add one.		

Privacy Specialists New

Name	Start Date	End Date
James Wilson	01/24/2005	

Request Routing Contacts New

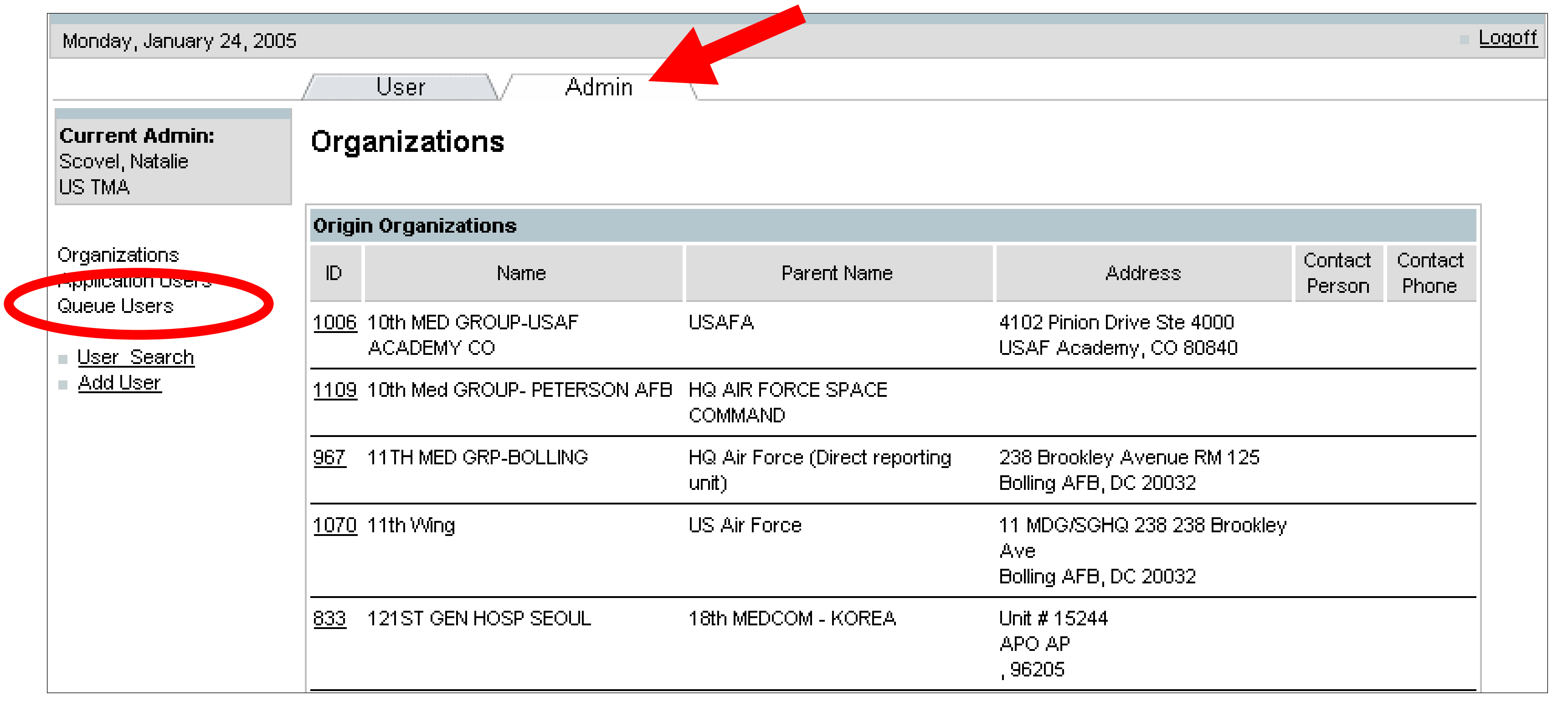
Name	Start Date	End Date
There are no Request Routing Contacts configured. Click new to add one.		

Queue Setup (1 of 8)

- A queue is a distribution list for a specific organization that is comprised of two or more Privacy Specialists
- The User Admin at the local command sets up queues
- Queues are created to expedite the process of approving/denying a disclosure
- Only users affiliated with a given organization will see that organization's routing options

Queue Setup (2 of 8)

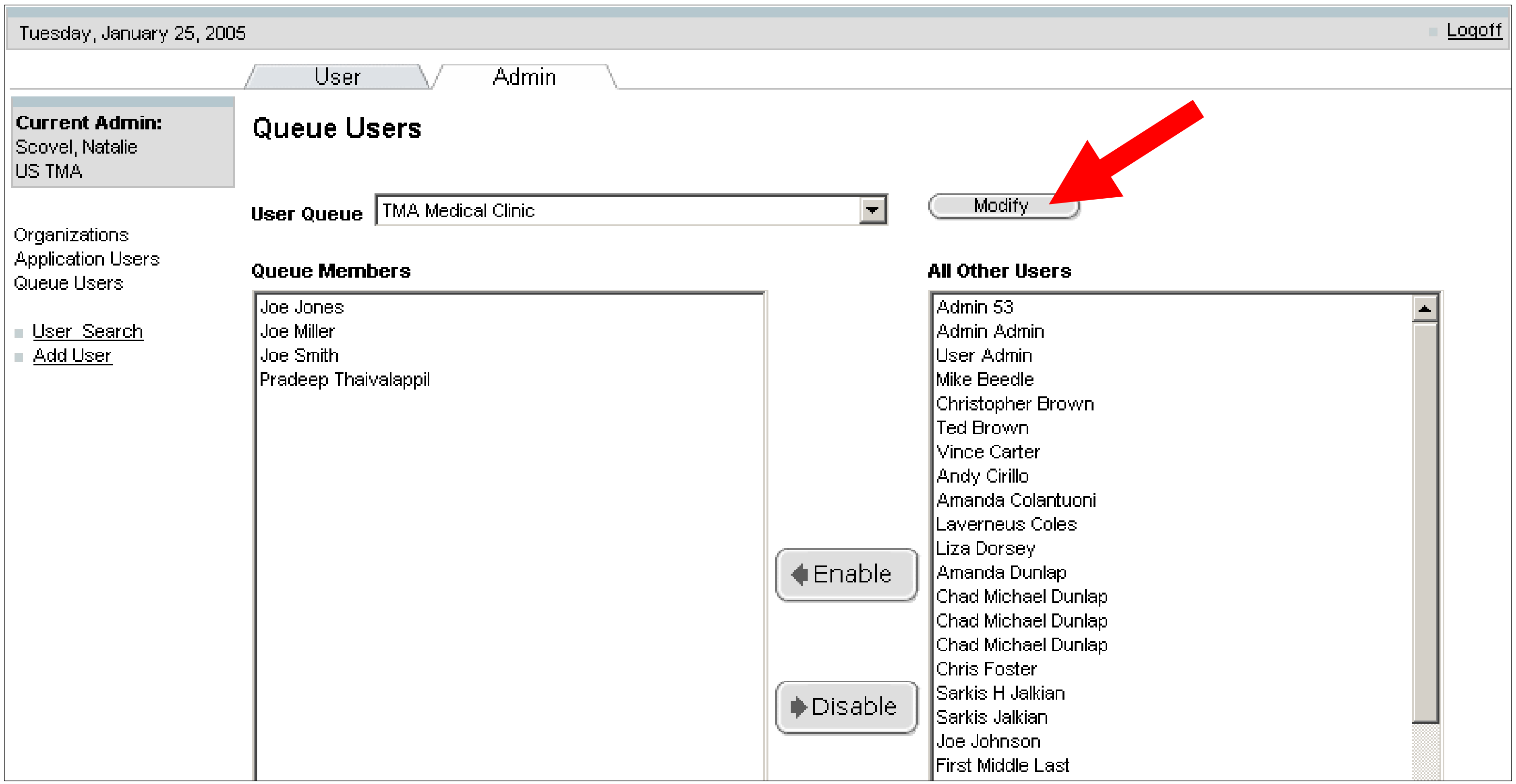
1. Select Admin Tab
2. Select the Queue Users hyperlink



User Admin Functionality

Queue Setup (3 of 8)

3. Click on the Modify button to add a new queue



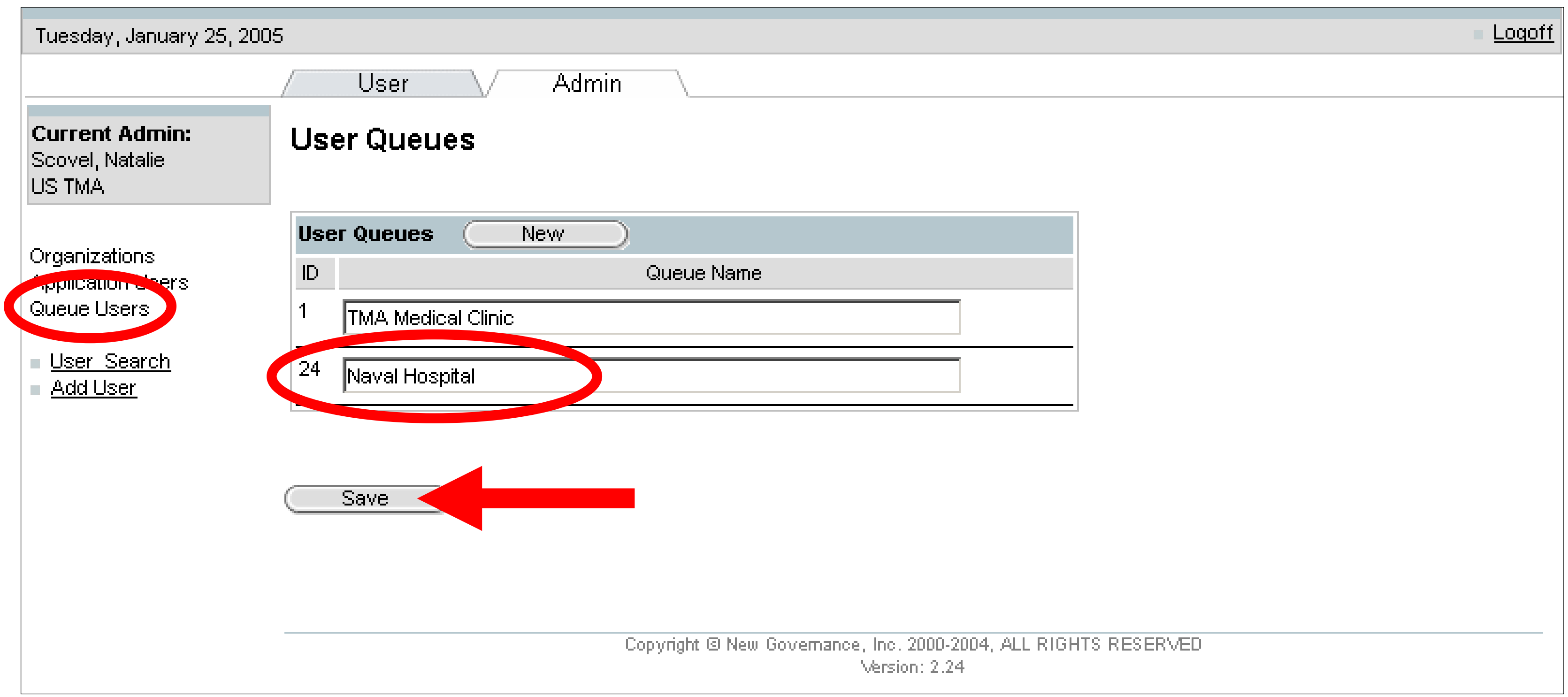
User Admin Functionality

Queue Setup (4 of 8)

4. Click on New

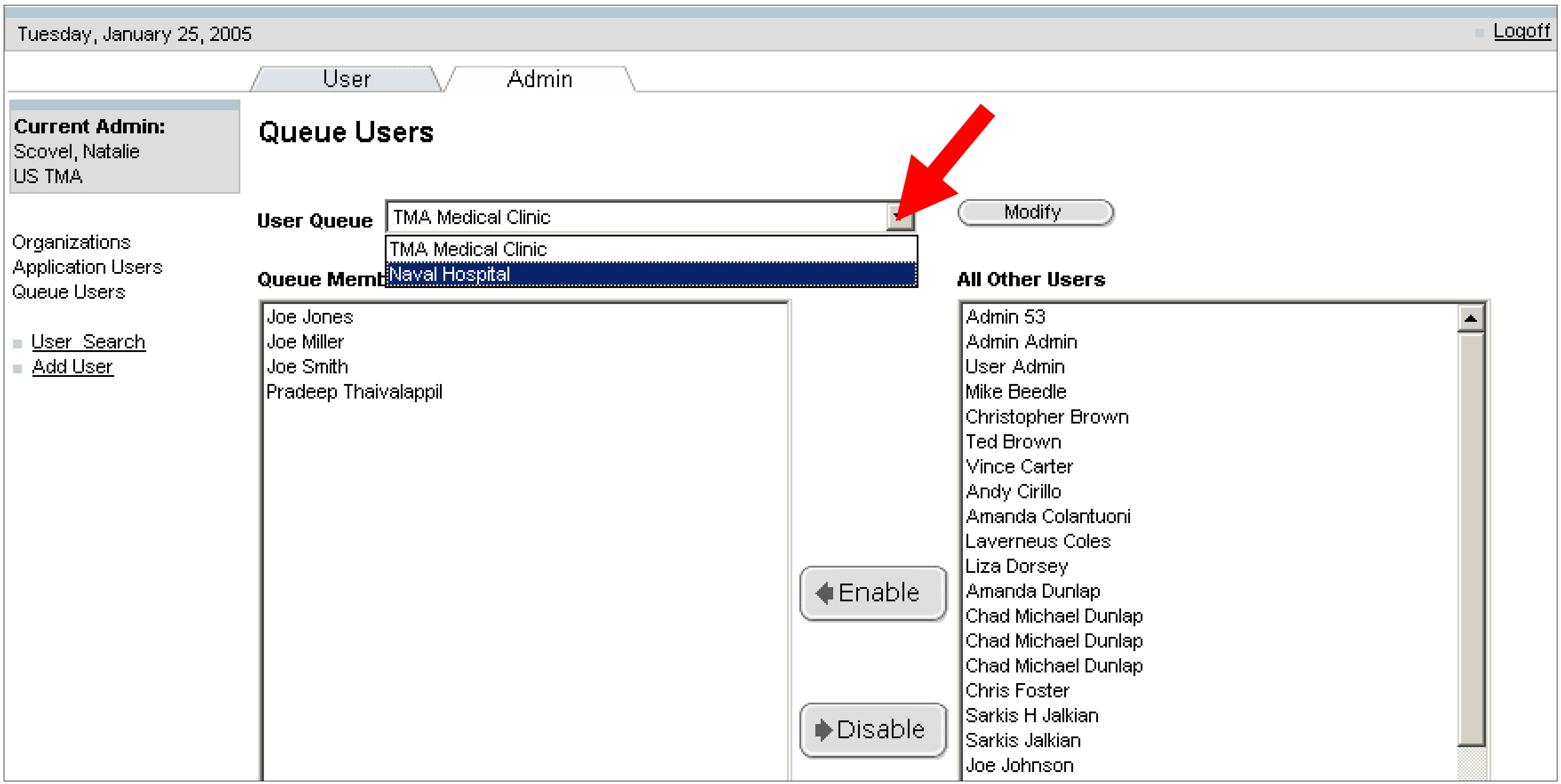
Queue Setup (5 of 8)

5. Enter the description of Queue in the text box
6. Click on the Save button (screen will not change)
7. Once saved, select the Queue Users hyperlink



Queue Setup (6 of 8)

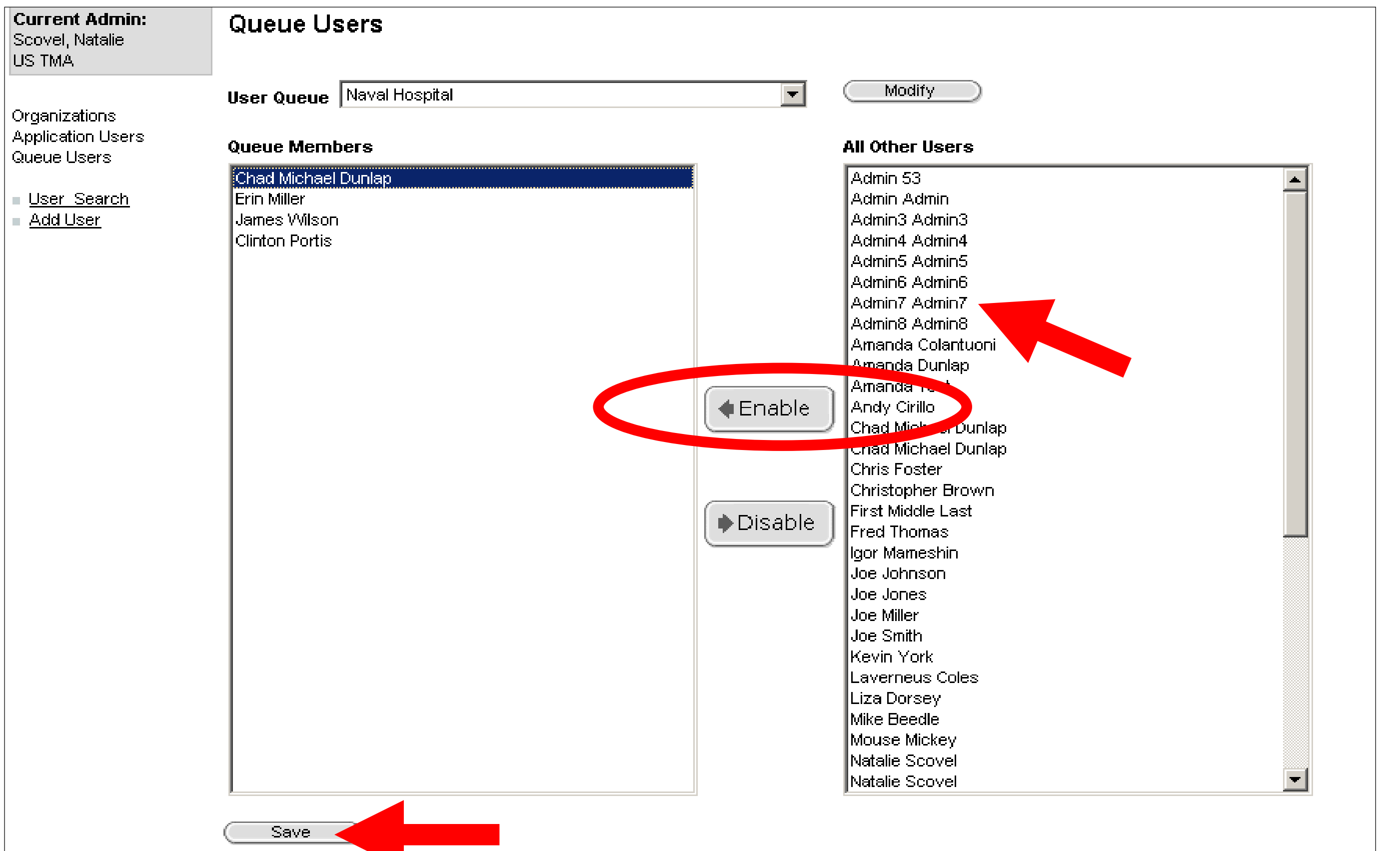
8. Select the Queue you created from the drop-down box



Queue Setup (7 of 8)

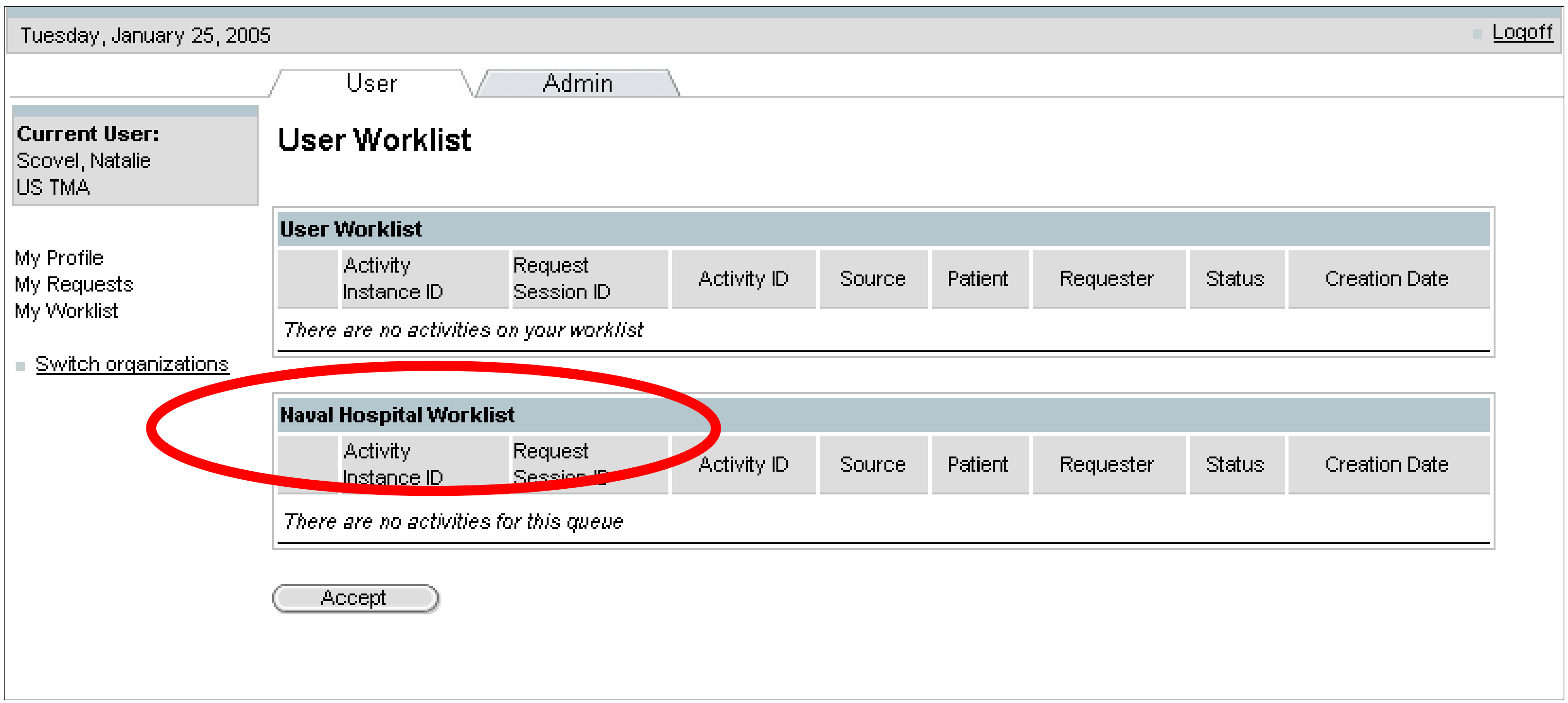
9. Select the users that you want to add to the queue and click on Enable

10. Click on the Save button



Queue Setup (8 of 8)

11. The Queue that you added will show up in the user's worklist



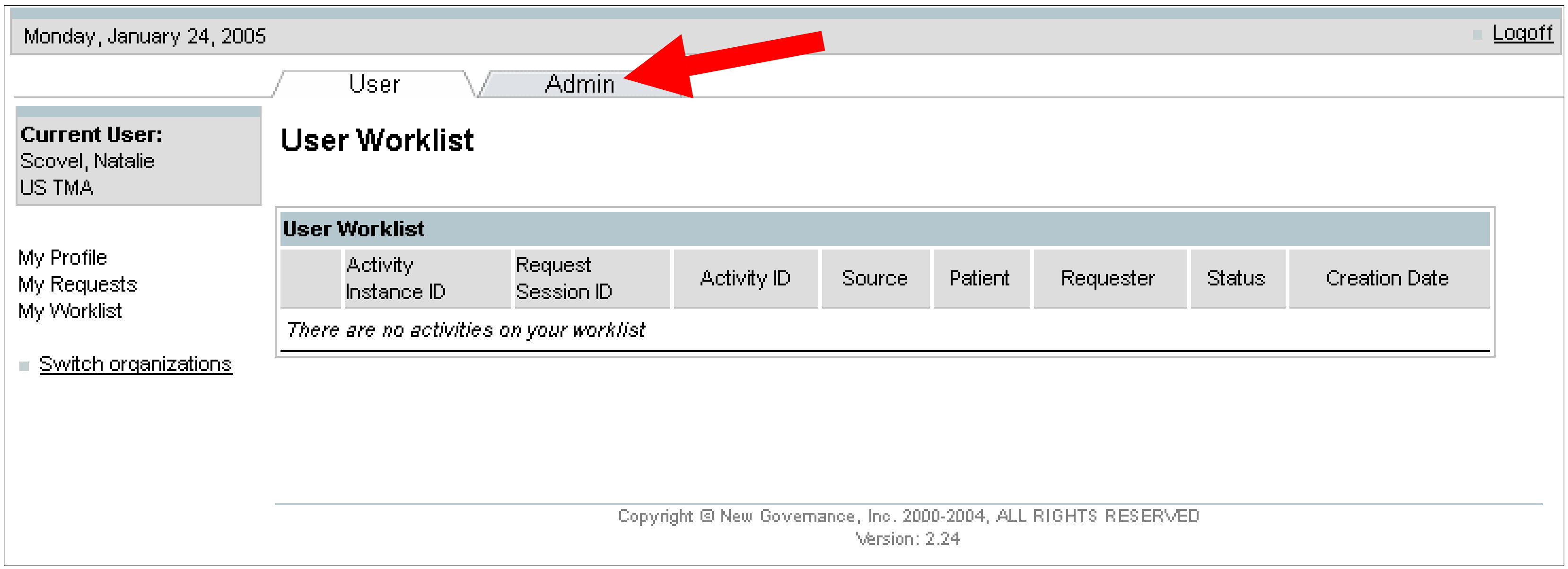
User Admin Functionality

Requester Favorites

- An organization can create a list of requester "favorites" that show up in the requester drop-down list box
- User Admins can set up the list of favorites per organization
- If an organization name is not in the favorites list, the user will be allowed to search for it manually
- A given "requester" can appear in multiple "favorites" lists

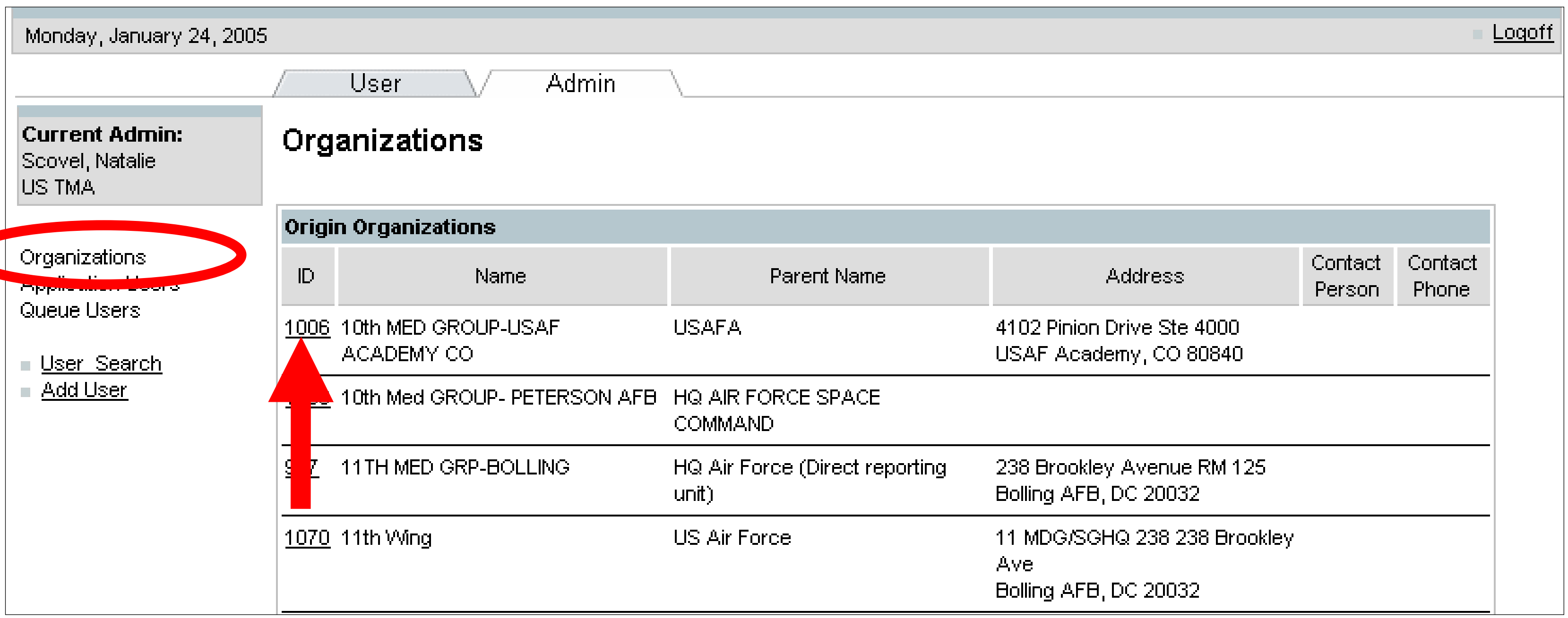
Requester Favorites- Searching for Organization (1 of 5)

1. Select the Admin Tab



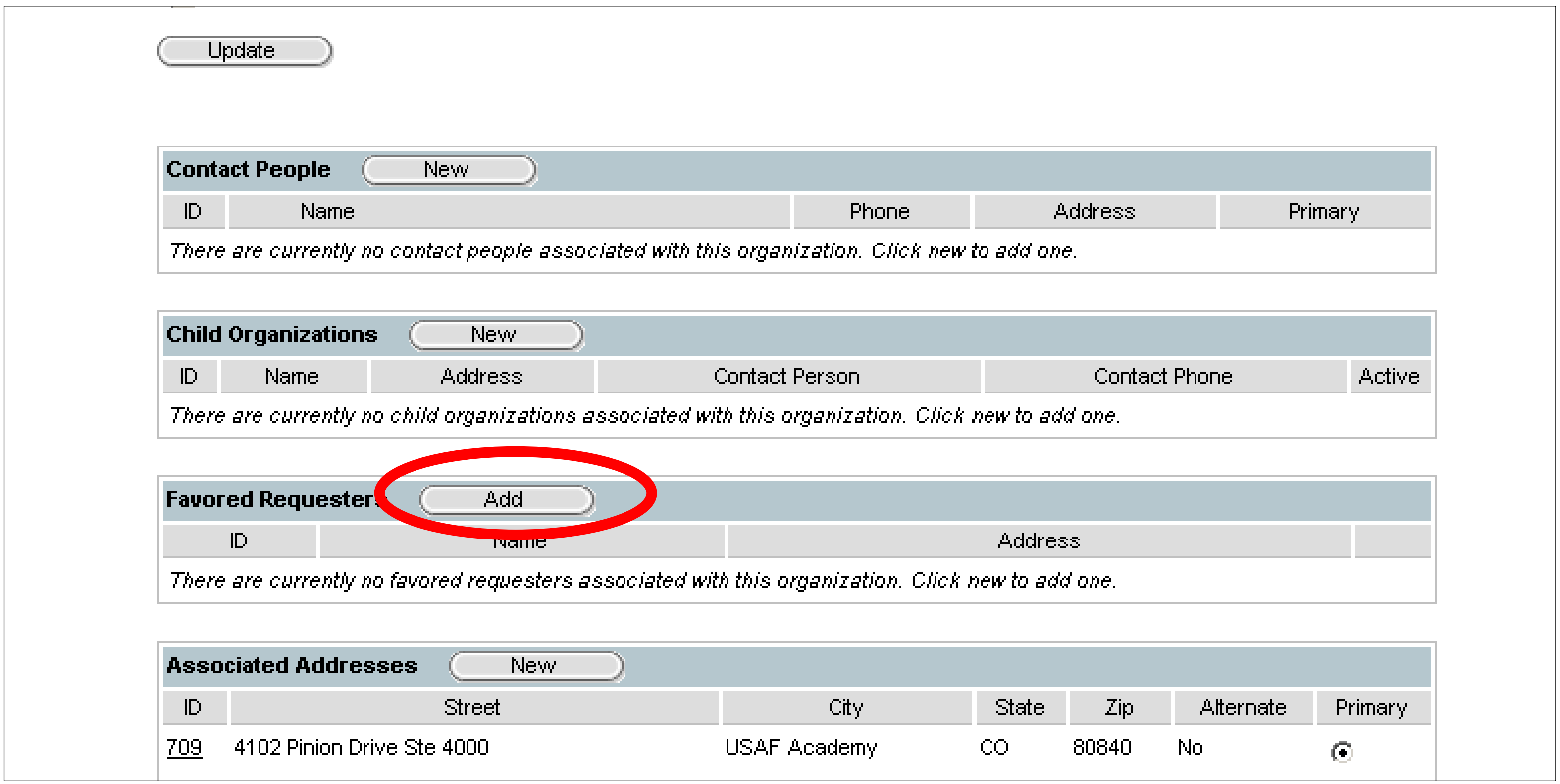
Requester Favorites- Searching for Organization (2 of 5)

2. Select the Organizations hyperlink
3. Select the ID hyperlink for your Origin Organization



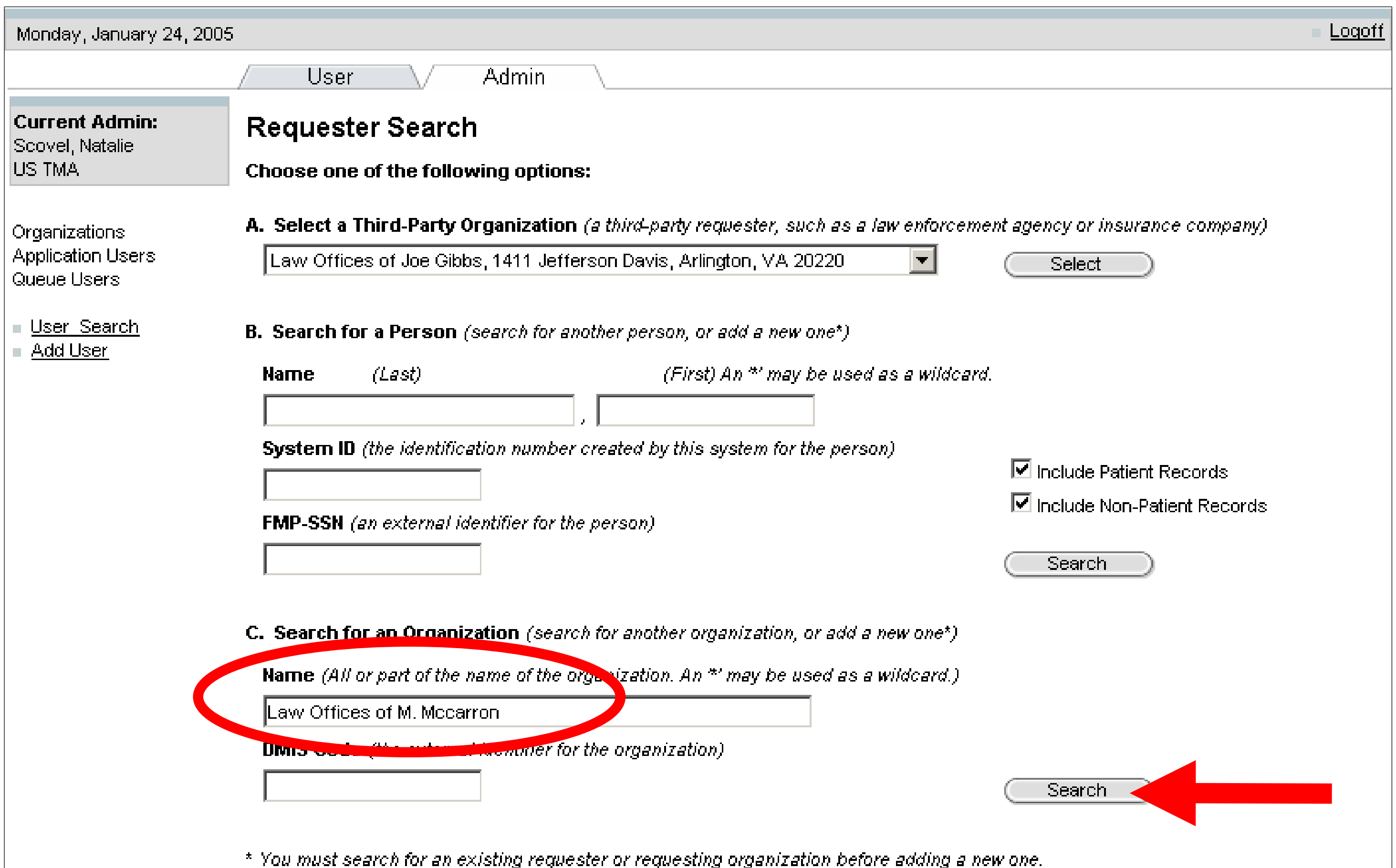
Requester Favorites- Searching for Organization (3 of 5)

4. Scroll down to Favored Requesters and click on the Add button



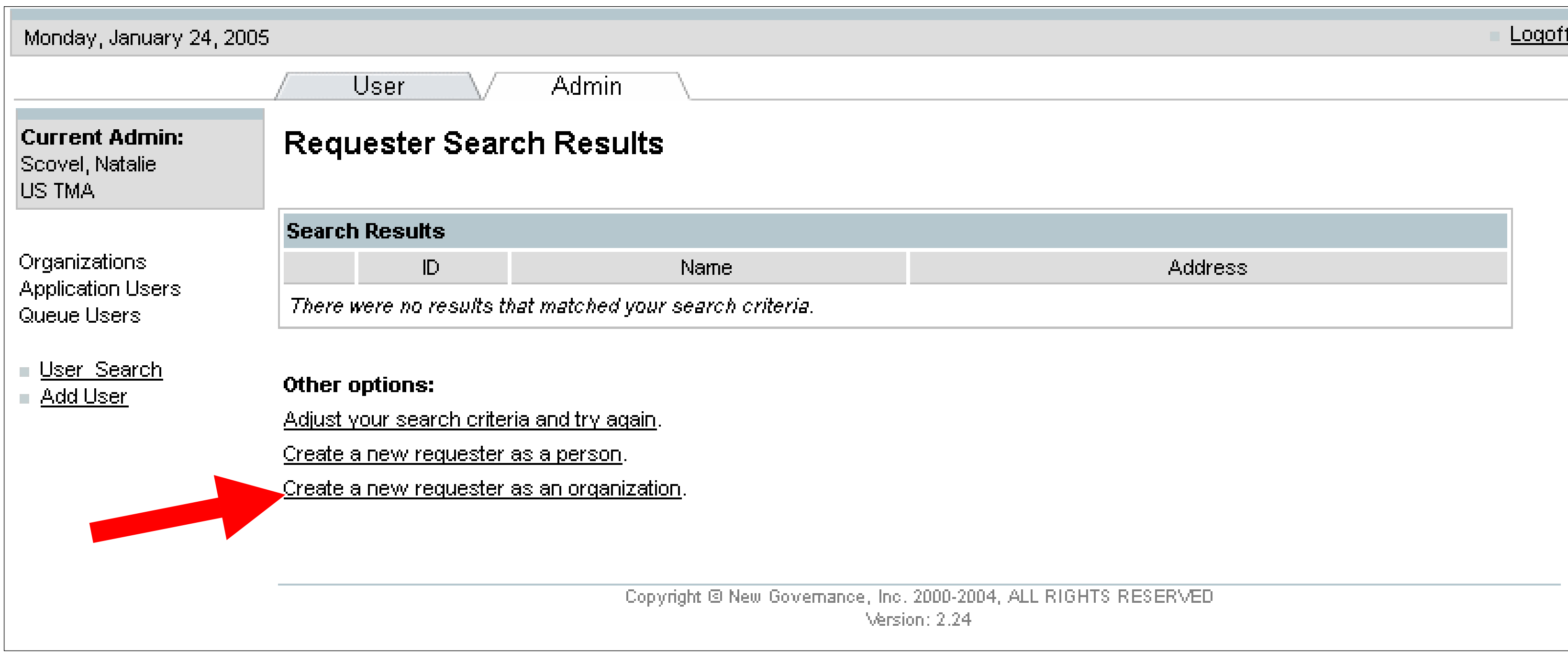
Requester Favorites- Searching for Organization (4 of 5)

5. Enter organization search criteria
6. Click on the Search button



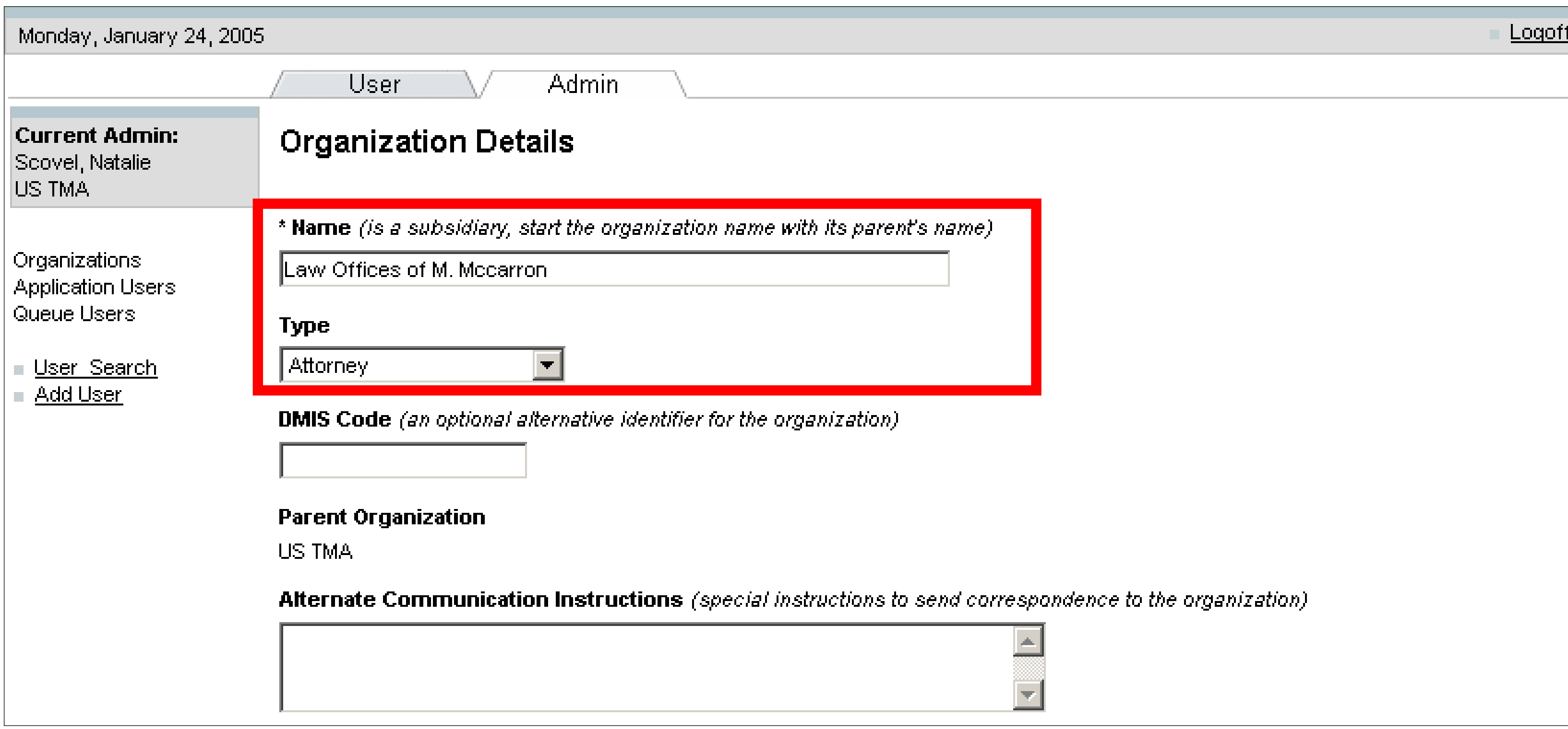
Requester Favorites- Searching for Organization (5 of 5)

7. If requester is not found, click on "Create a new requester as an organization"



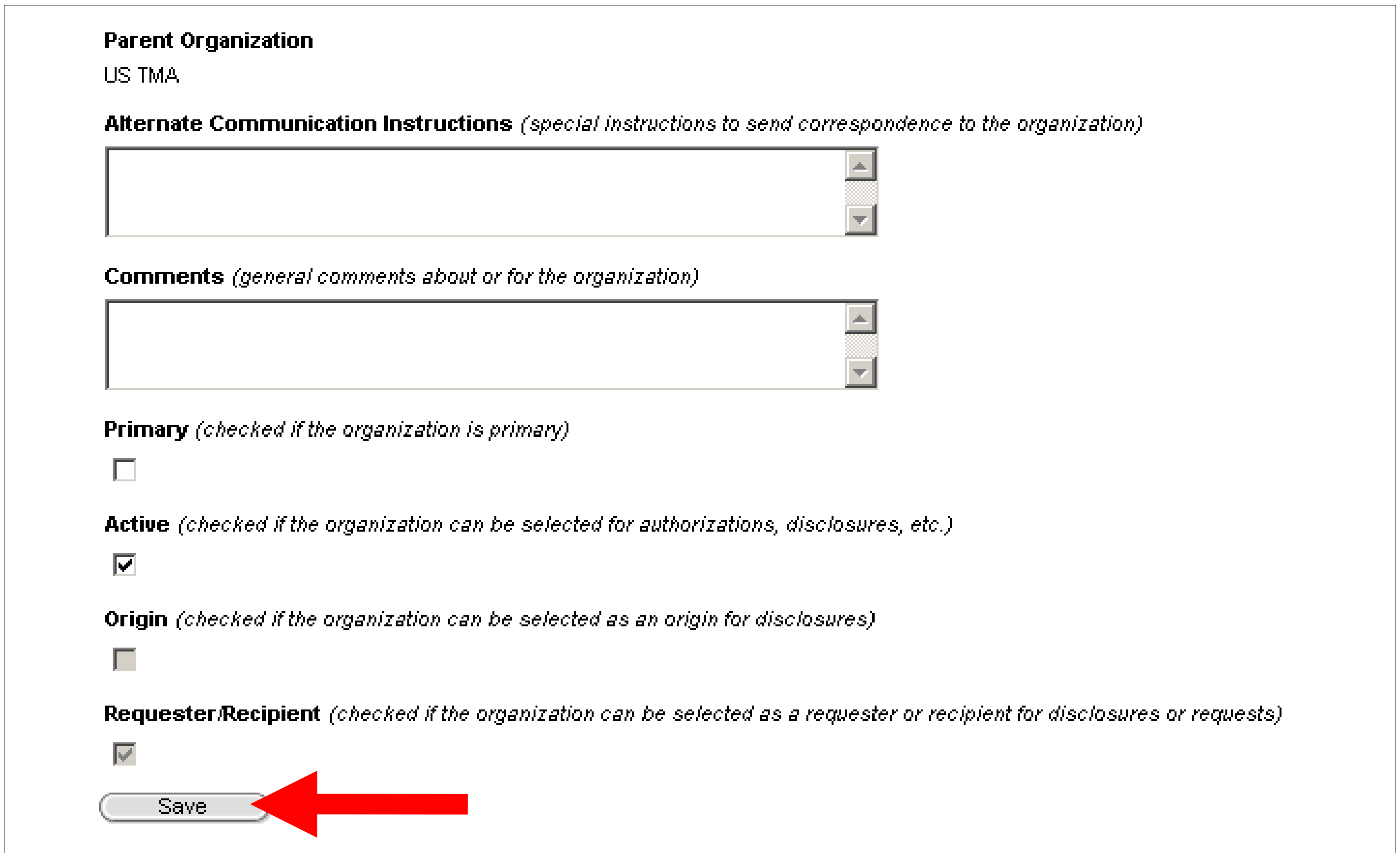
Requester Favorites- Adding New Organization (1 of 6)

8. Enter the name of the Organization
9. Select the organization type from the drop-down box



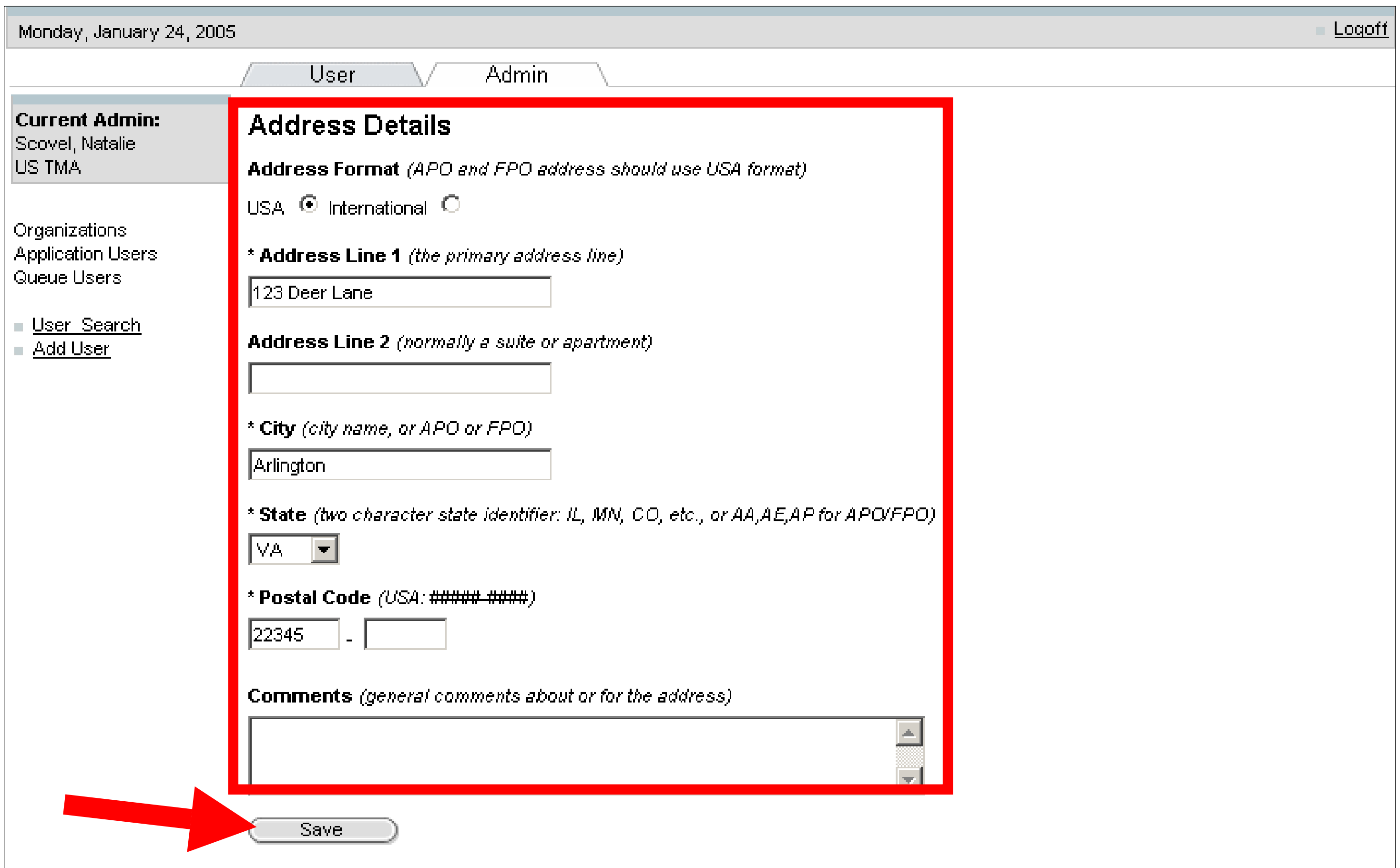
Requester Favorites- Adding New Organization (2 of 6)

10. Scroll down to the bottom of the screen and click on the Save button



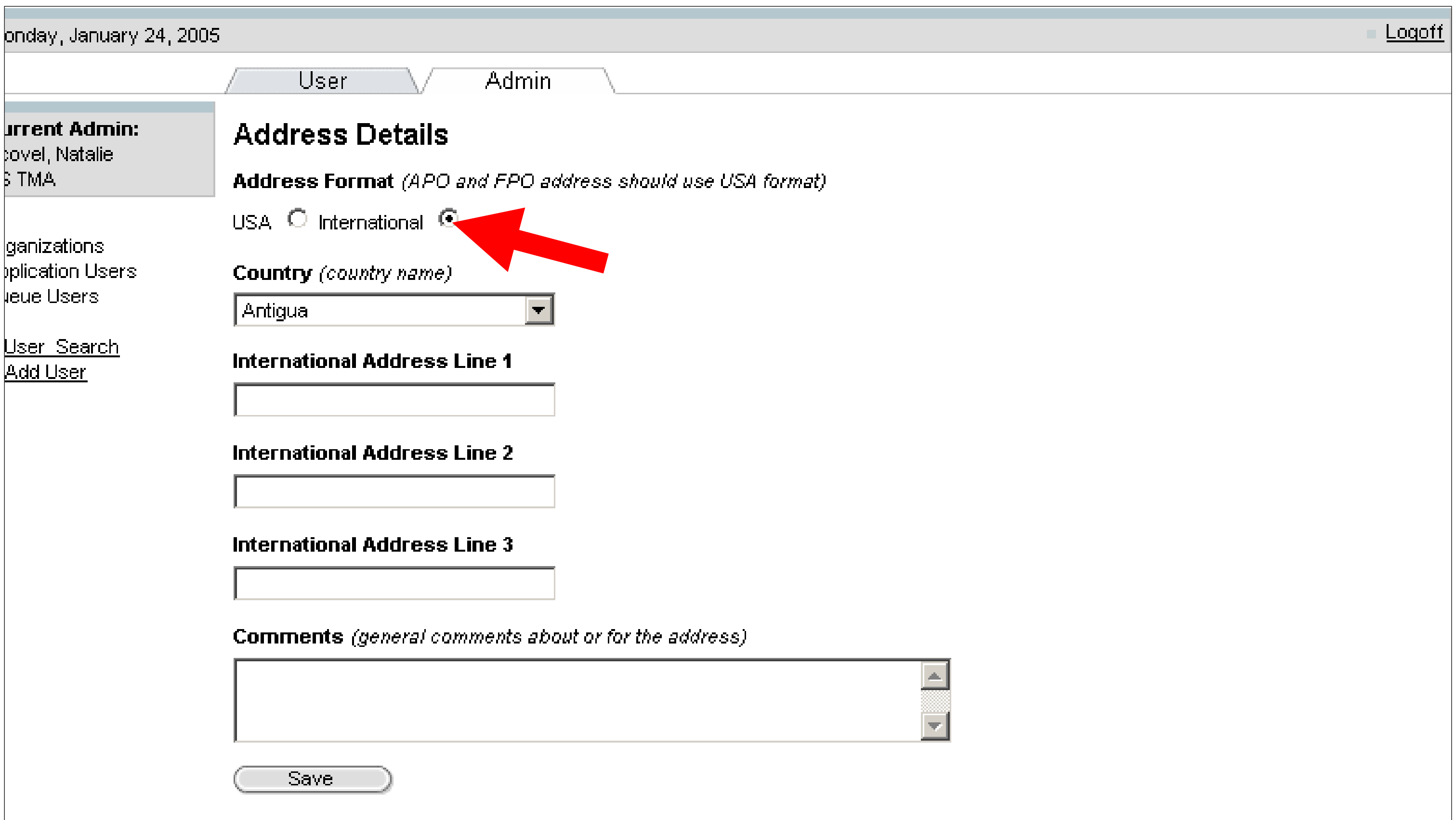
Requester Favorites- Adding New Organization (3 of 6)

11. Enter the Organization Address Details and click on the Save button



Requester Favorites- Adding New Organization (4 of 6)

- If you are entering a International address, select the International radio button



Requester Favorites- Adding New Organization (5 of 6)

- The organization that you added now appears in your requester favorites

Update

Contact People New

ID	Name	Phone	Address	Primary

There are currently no contact people associated with this organization. Click new to add one.

Child Organizations New

ID	Name	Address	Contact Person	Contact Phone	Active

There are currently no child organizations associated with this organization. Click new to add one.

Favored Requesters Add

ID	Name	Address	
1220	Law Offices of M. Mccarron	123 Deer Ln., Arlington, VA 22345	remove

Associated Addresses New

ID	Street	City	State	Zip	Alternate	Primary
709	4102 Pinion Drive Ste 4000	USAF Academy	CO	80840	No	⦿

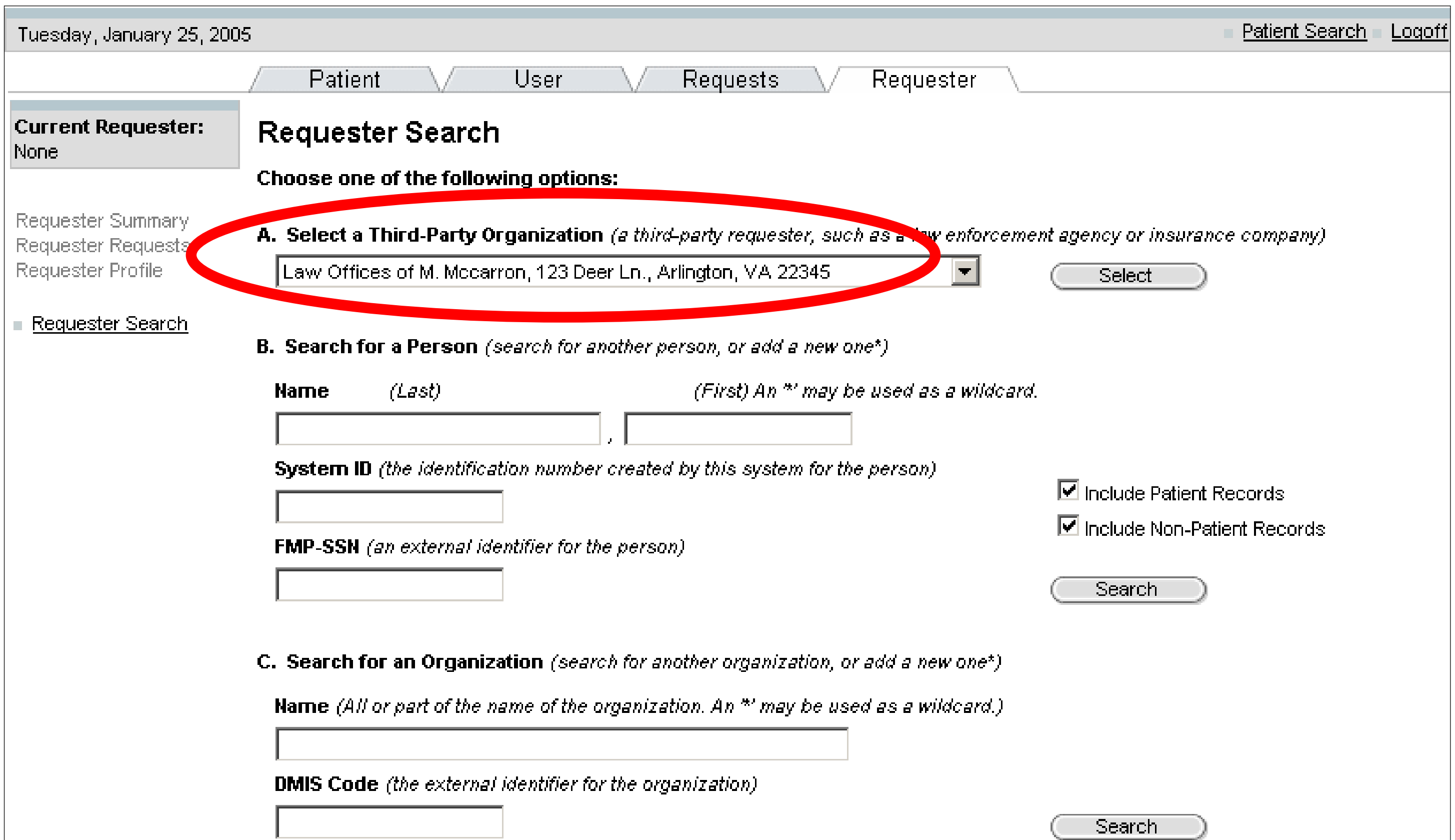
Phone Numbers New

ID	Phone	Comment	Active	Primary

There are currently no phone numbers on record for this organization. Click new to add one.

Requester Favorites- Adding New Organization (6 of 6)

- When logging in as a Regular User, the organization you added will appear in the requester drop-down box for your organization



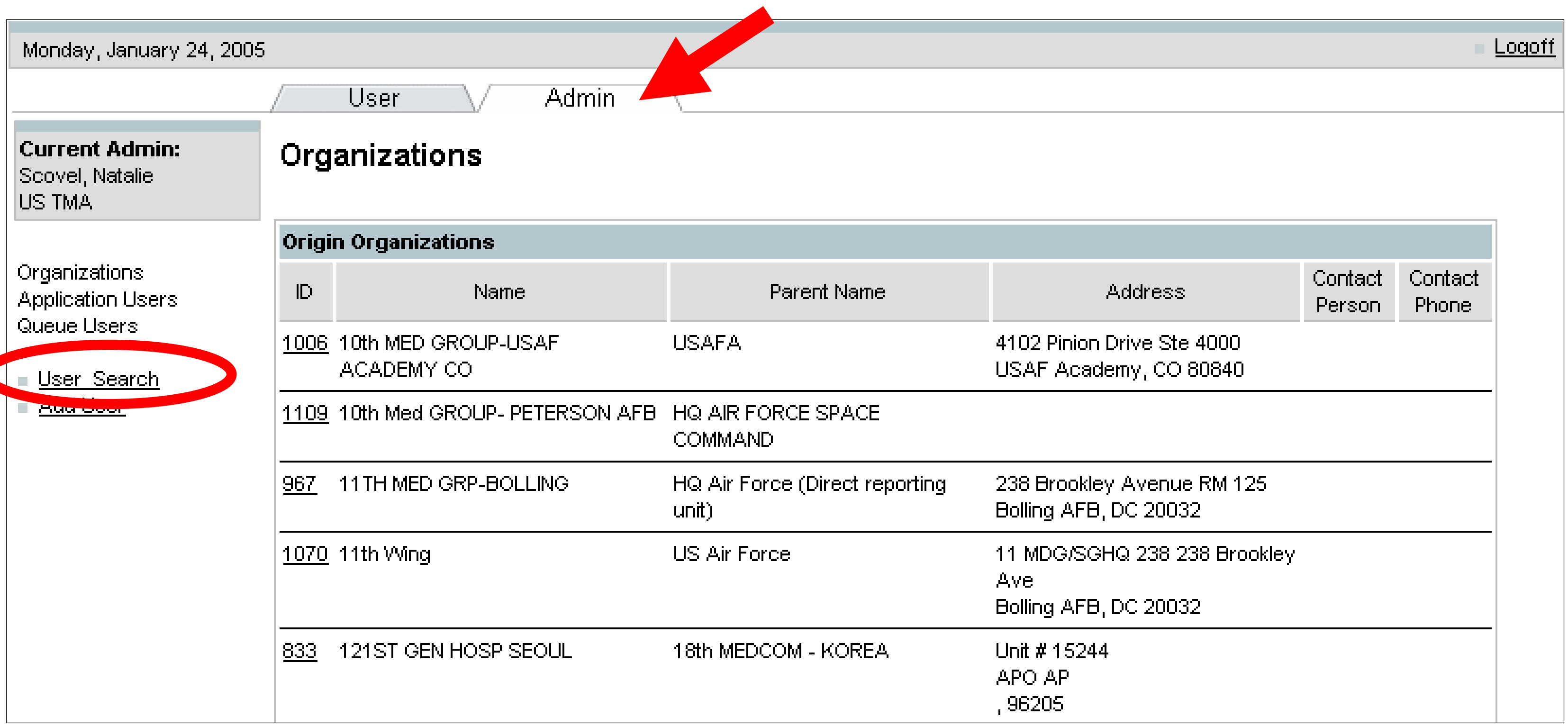
User Admin Functionality

Disabling Users (1 of 5)

- If a user transfers to another facility or separates from the Service, the User Admin needs to disable that individual's ability to access the tool
- You cannot delete users from the system
  - Future auditing
  - Disclosures tracking
  - Users are attached to records they created

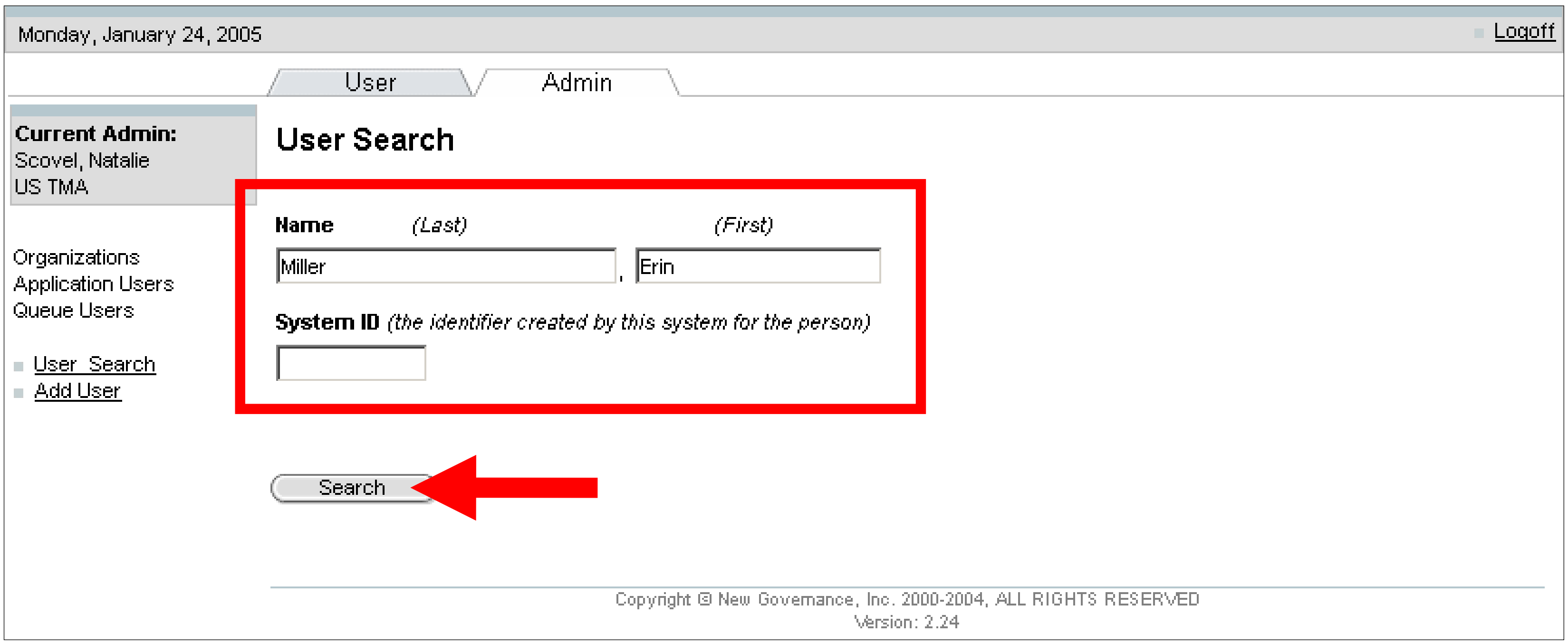
Disabling Users (2 of 5)

1. Select the Admin Tab
2. Select the User Search hyperlink



Disabling Users (3 of 5)

3. Enter search criteria
4. Click on the Search button

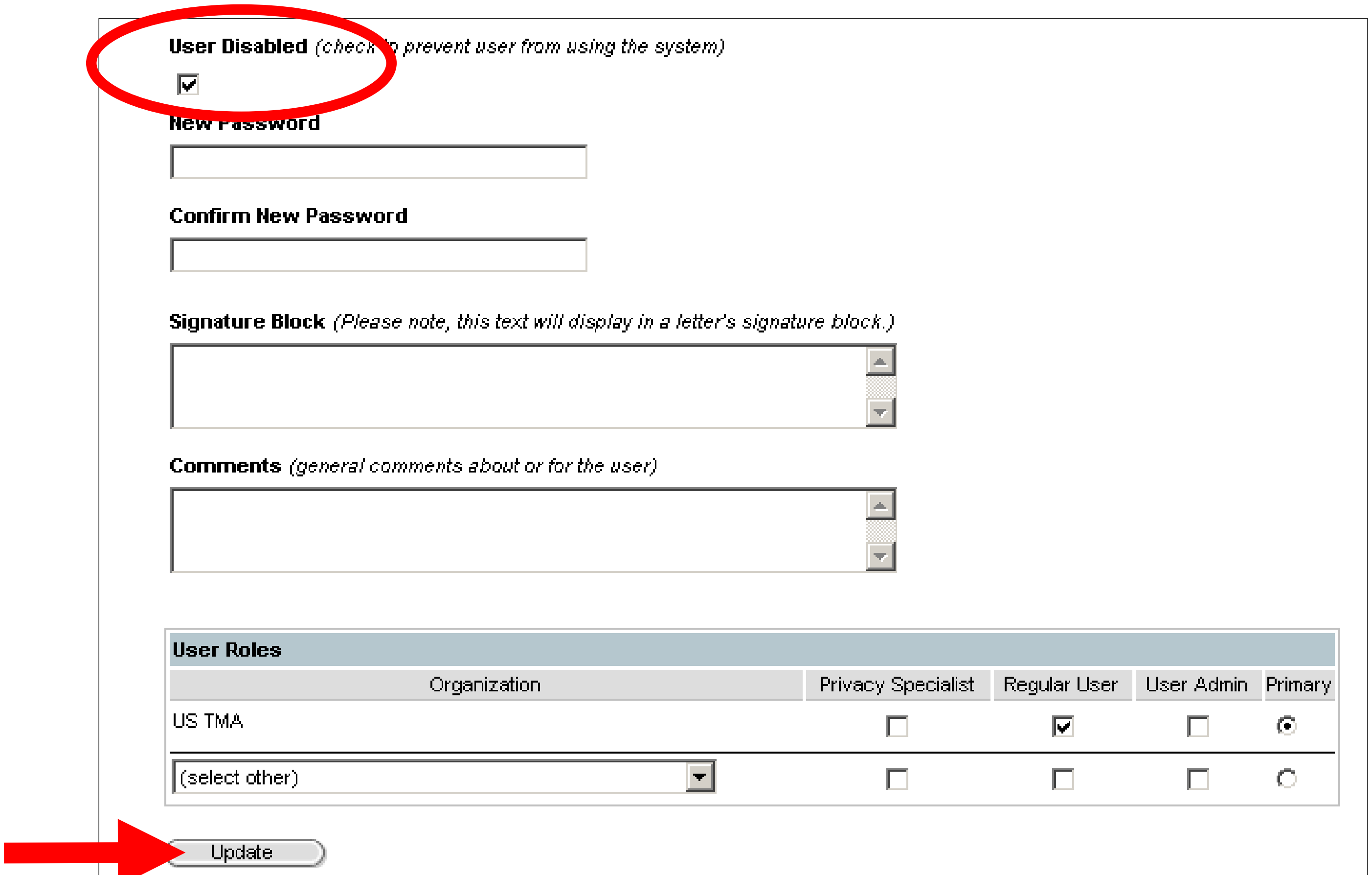


Disabling Users (4 of 5)

5. Click on the radio button next to the user to be disabled
6. Click on the Select button

Disabling Users (5 of 5)

7. Scroll down and place a check in the "User Disabled" box
8. Click on the Update button



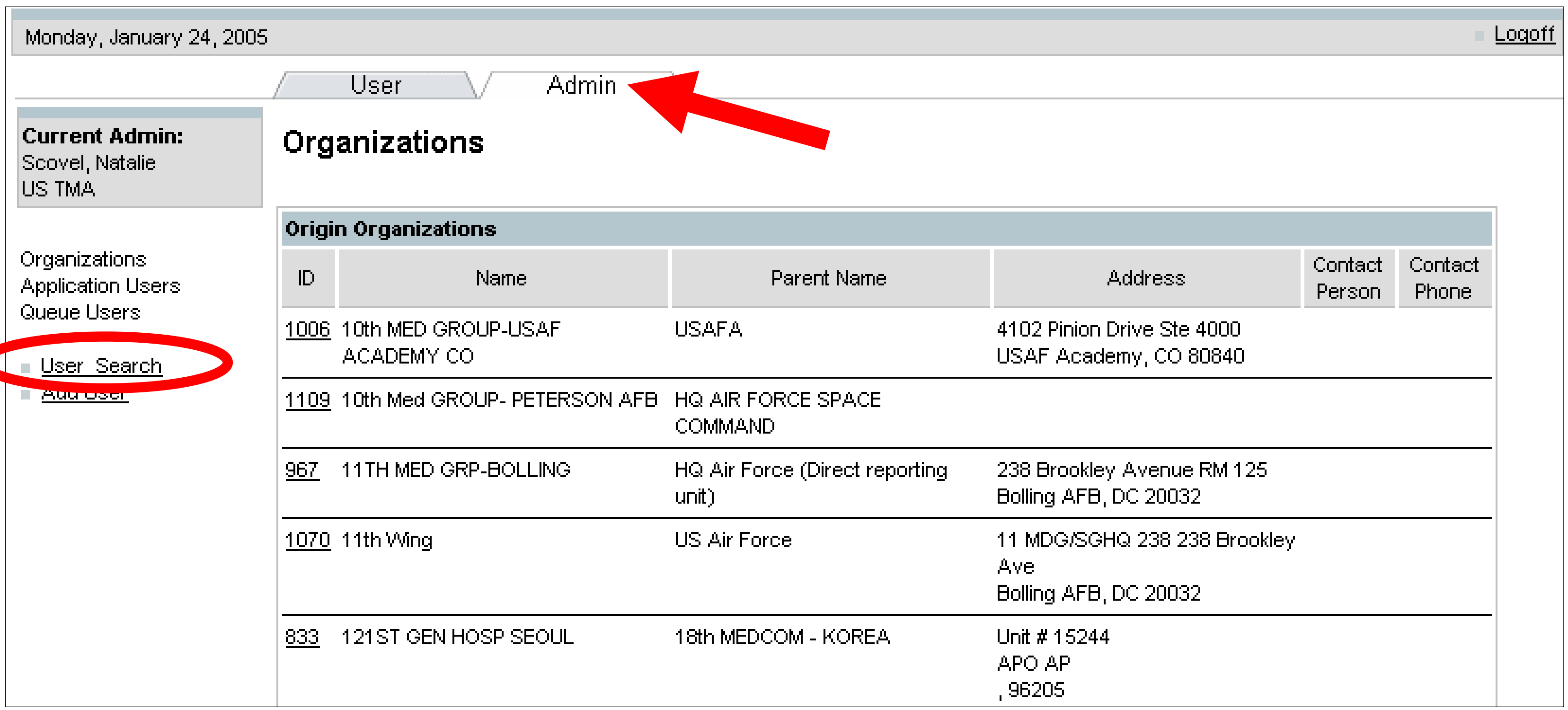
User Admin Functionality

Transferring Users (1 of 6)

- A transfer from one MTF to another can only be executed by the User Admin at the Service level
- If a user transfers to a new organization, the User Admin at the receiving location would initiate an action for the transfer according to Service requirements
- If a User transfers from one Service to another, please contact the HIPAA Support Center at
  - Hipaasupport@tma.osd.mil
- The User Admin can only search for users within their level of the hierarchy

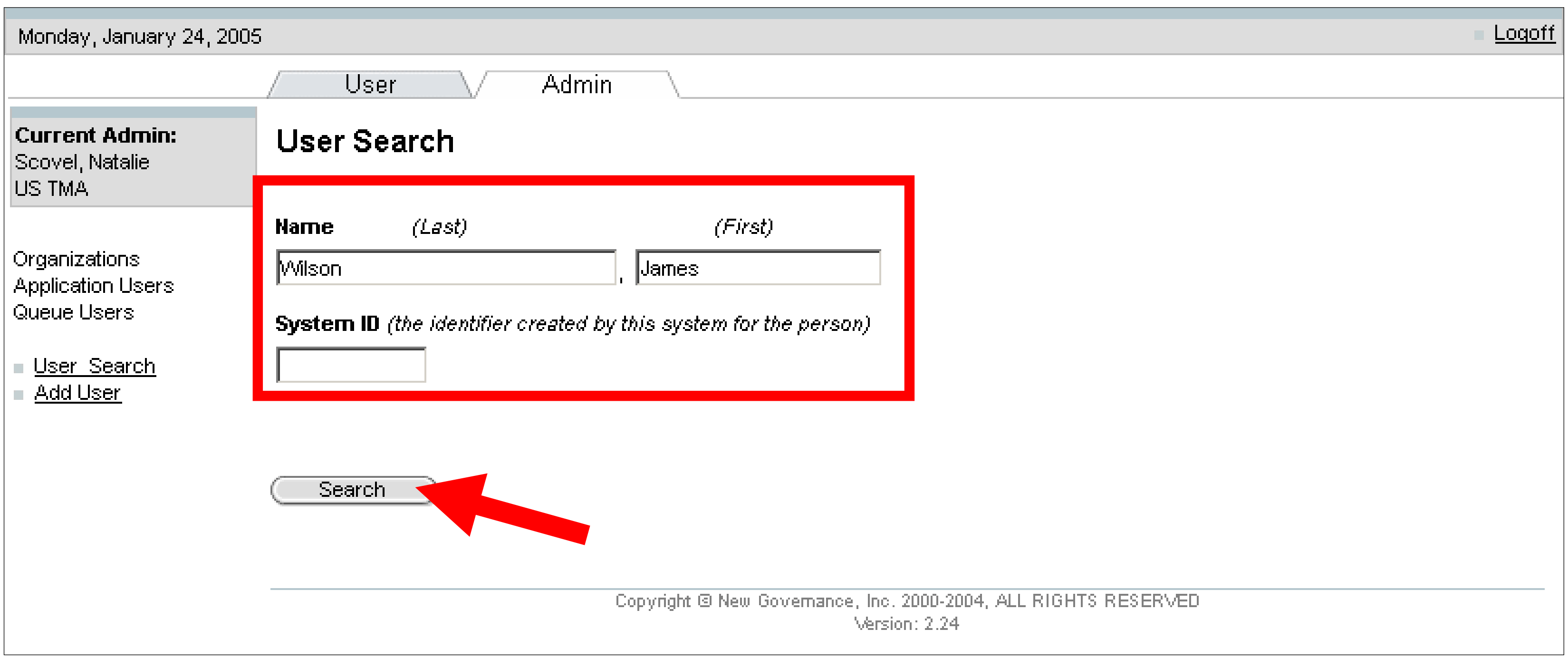
Transferring Users (2 of 6)

1. Select the Admin Tab
2. Select the User Search hyperlink



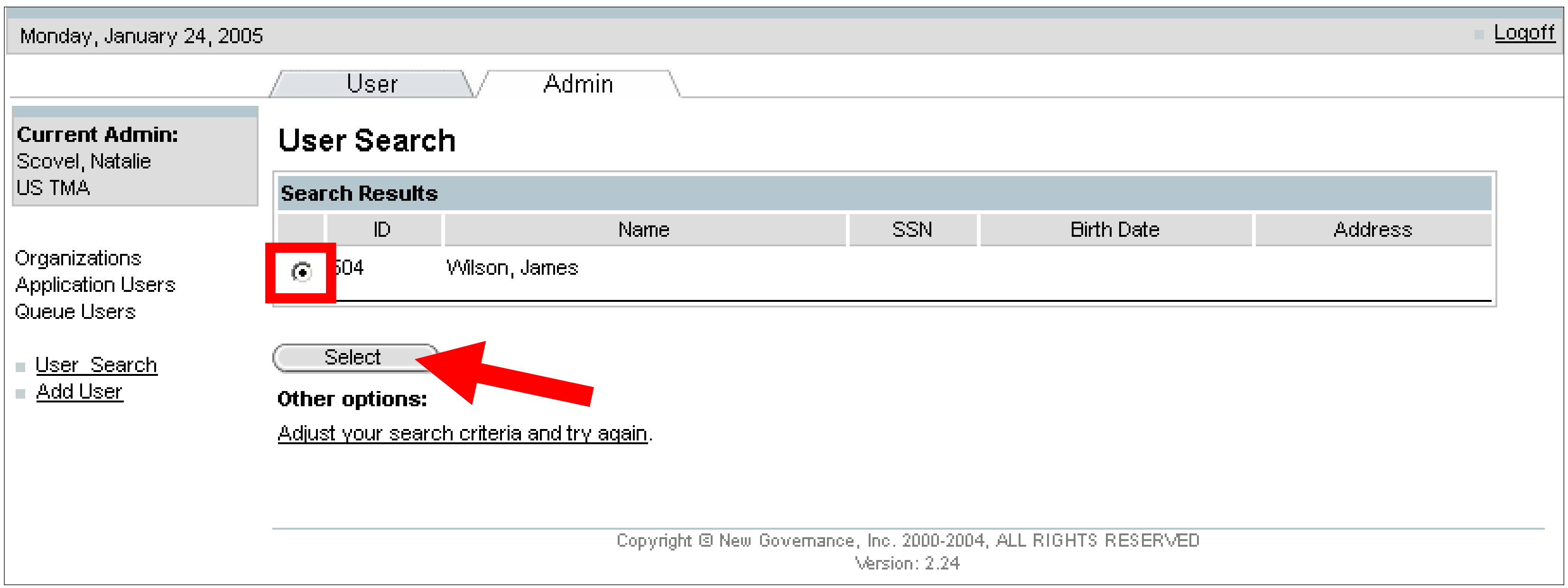
Transferring Users (3 of 6)

3. Enter the search criteria
4. Click on the Search button



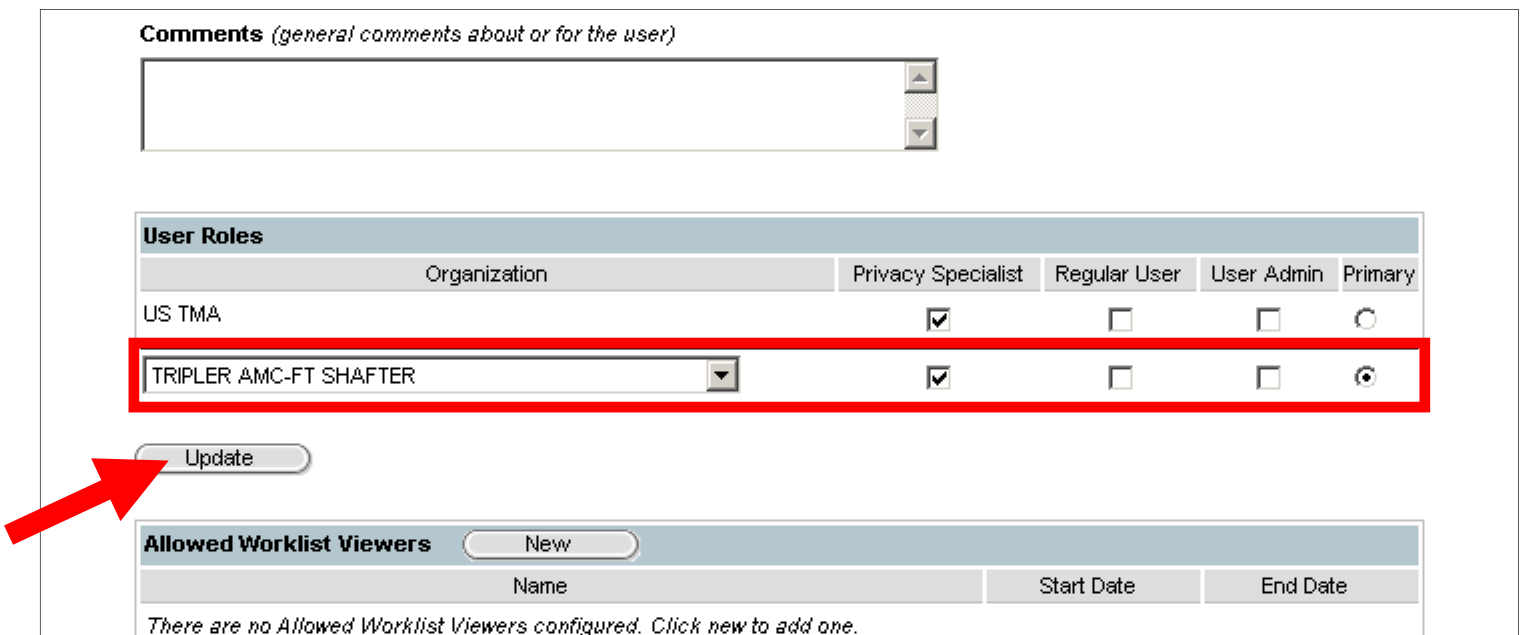
Transferring Users (4 of 6)

5. Click on the radio button for the user to be transferred
6. Click on the Select button



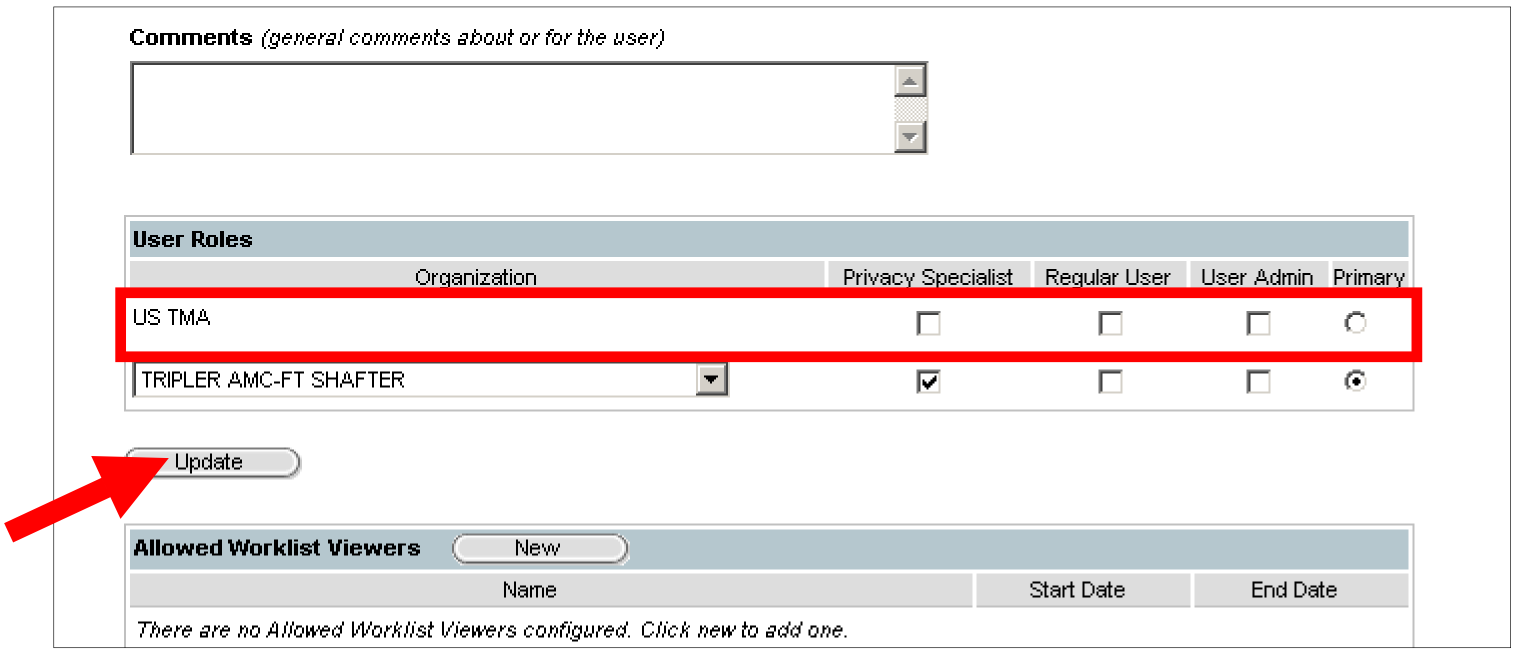
Transferring Users (5 of 6)

7. Scroll down to the User Roles section
8. Select a new organization from the drop-down box and make any changes to the user role
9. Select primary radio button for the new organization
10. Click on the Update button



Transferring Users (6 of 6)

11. Remove the check for the old organization and role
12. Click on Update



Summary

- You should now be able to:
  - Describe the process of obtaining a User Admin account
  - Create user accounts
  - Setup a workflow
  - Setup a queue
  - Create requester favorites
  - Disable users
  - Transfer users

Privacy Specialist/Regular User Functionality

Objectives

- Upon completion of this lesson, you will be able to perform the tool functions related to:
  - Patient Records
  - Disclosures
  - Accounting of Disclosures
  - Suspending Disclosures
  - Restrictions
  - Authorizations

Patient Records

Objectives

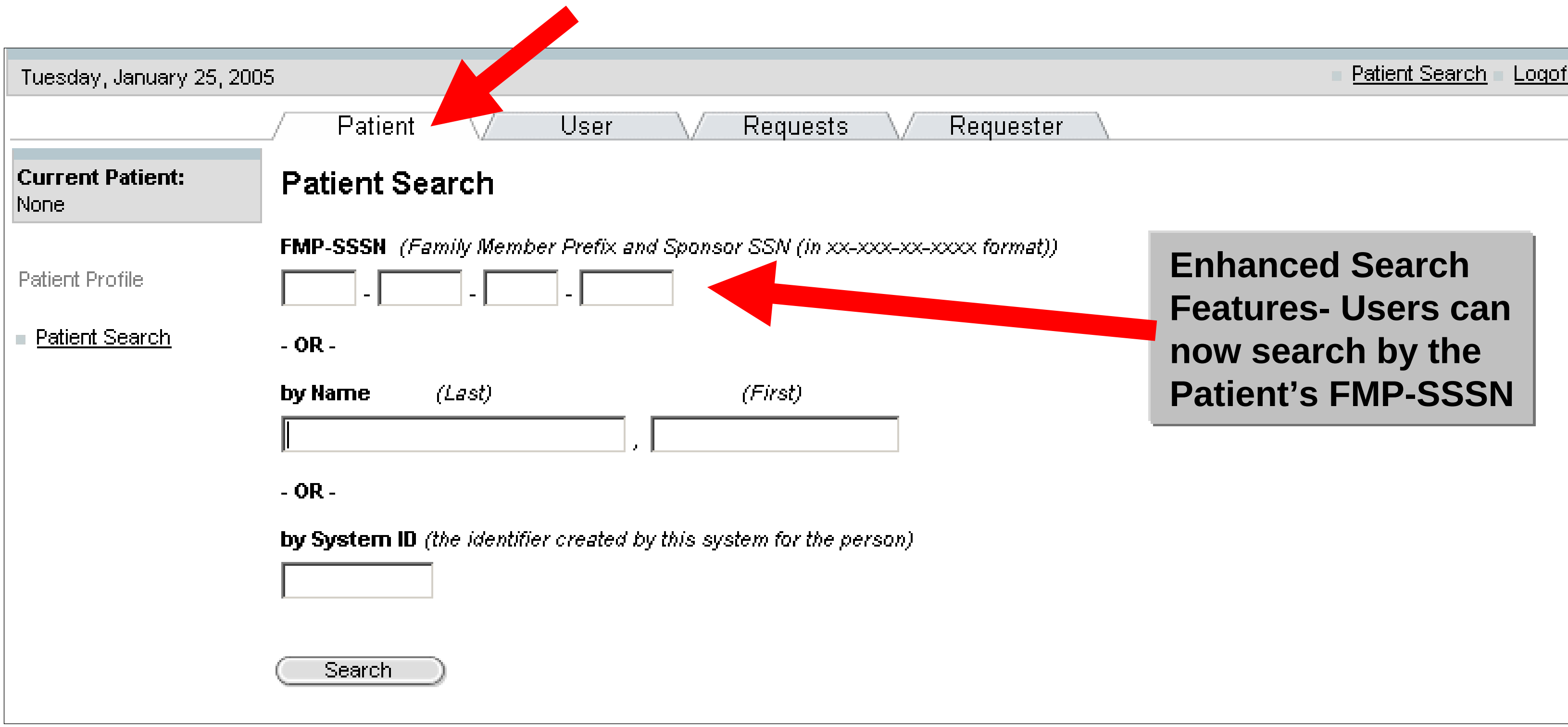
- Upon completion of this lesson, you will be able to:
  - Search for a patient record
  - Add a patient record
  - Create an alternative address
  - Create an alternative telephone number

Search for a Patient Record (1 of 4)

- The user must search for a patient record in order to:
  - Track a disclosure
  - Identify an authorization or restriction
  - Track a complaint
- The user can search for a patient record using the Family Member Prefix Sponsor's SSN (FMP-SSSN) or the patient's name
  - Partial searches are allowed
    - If you don't know the FMP
    - If you only know part of the Sponsor's SSN

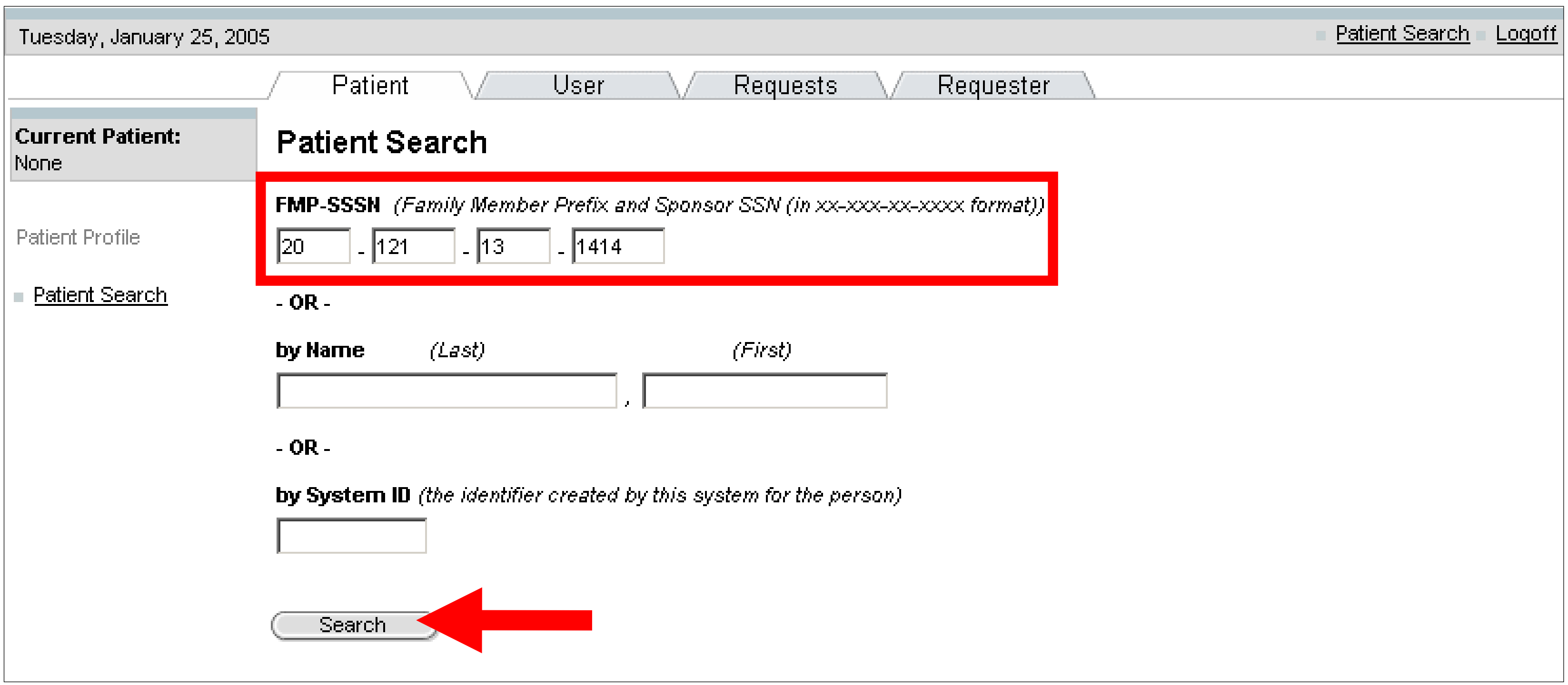
Search for a Patient Record (2 of 4)

1. Select the Patient Tab



Search for a Patient Record (3 of 4)

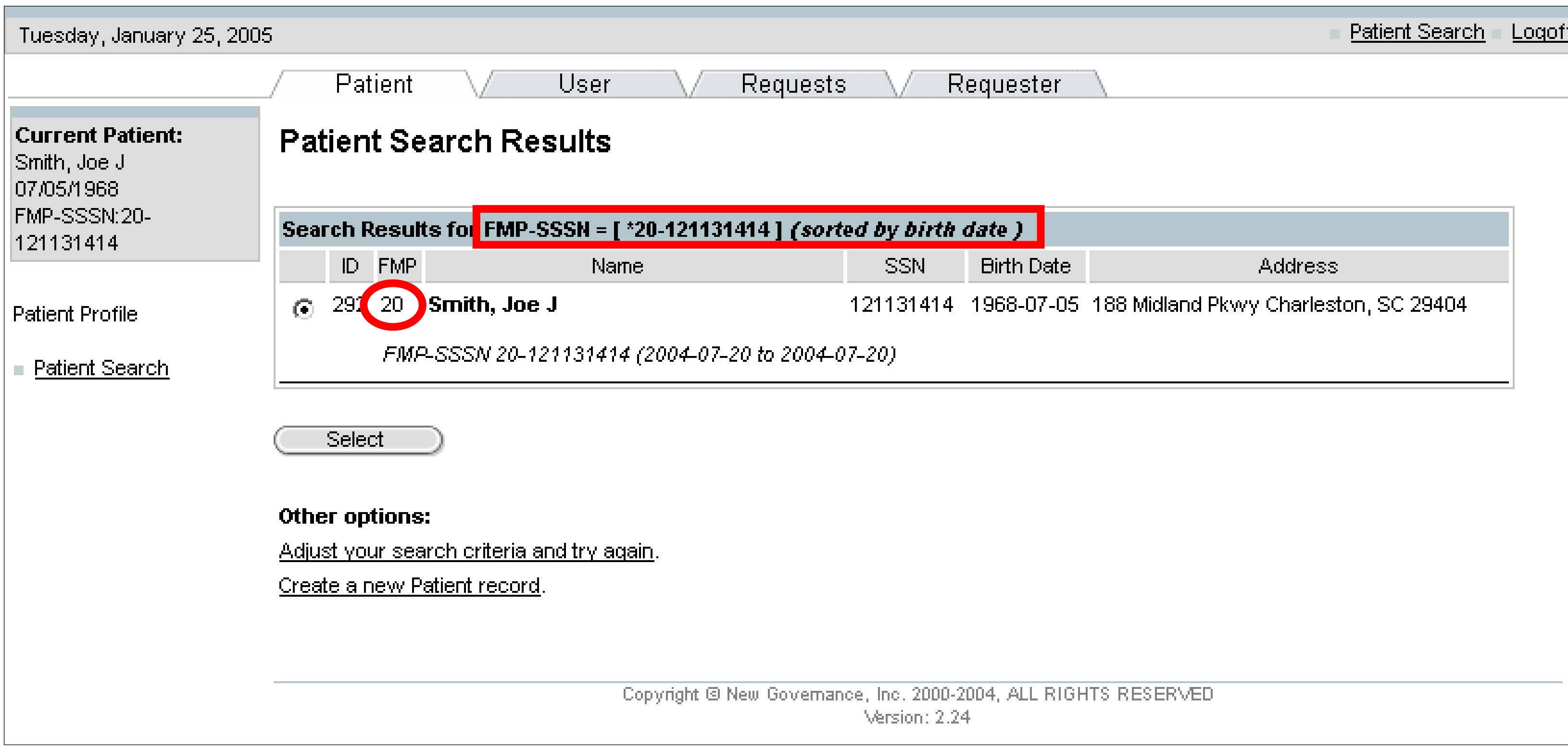
2. Type in the Search criteria (FMP-SSSN)
3. Click on the Search button



Patient Records

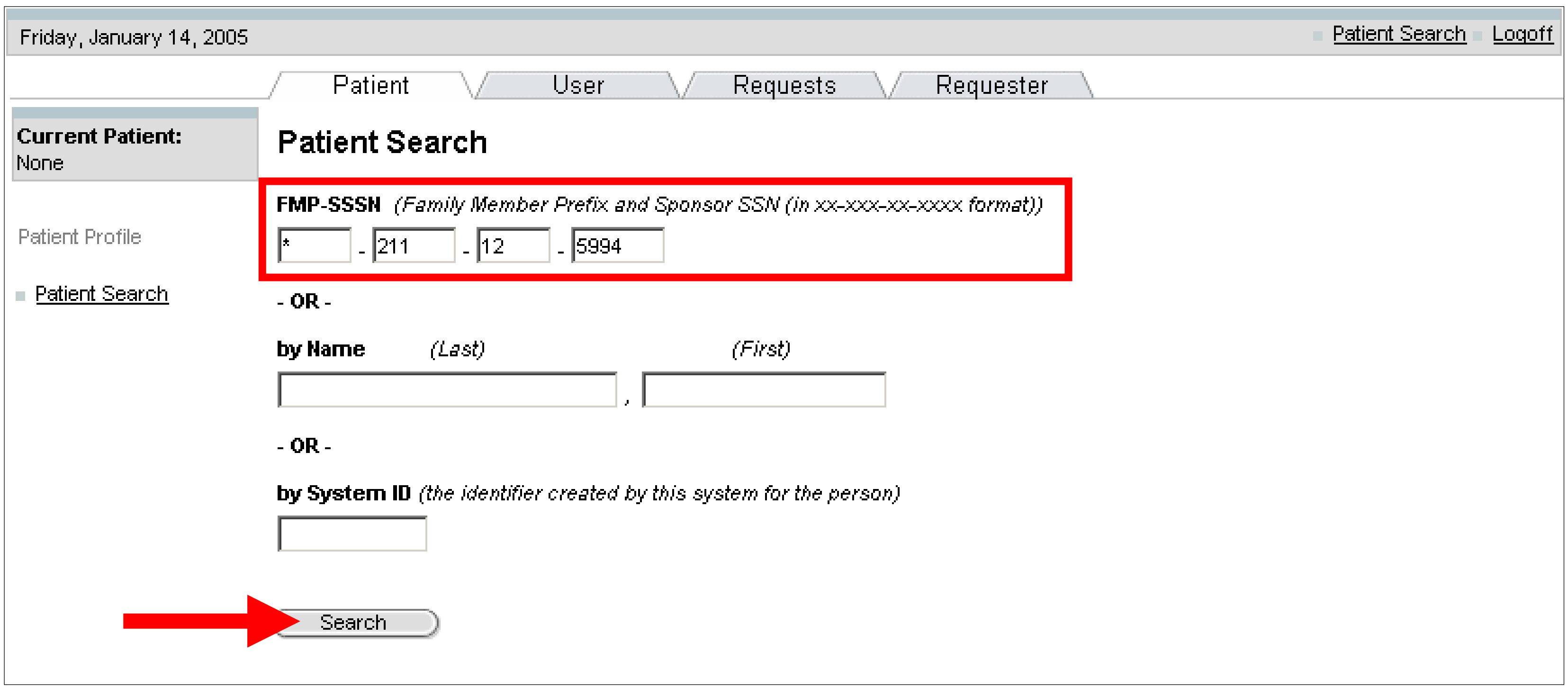
Search for a Patient Record (4 of 4)

4. Search Results will display



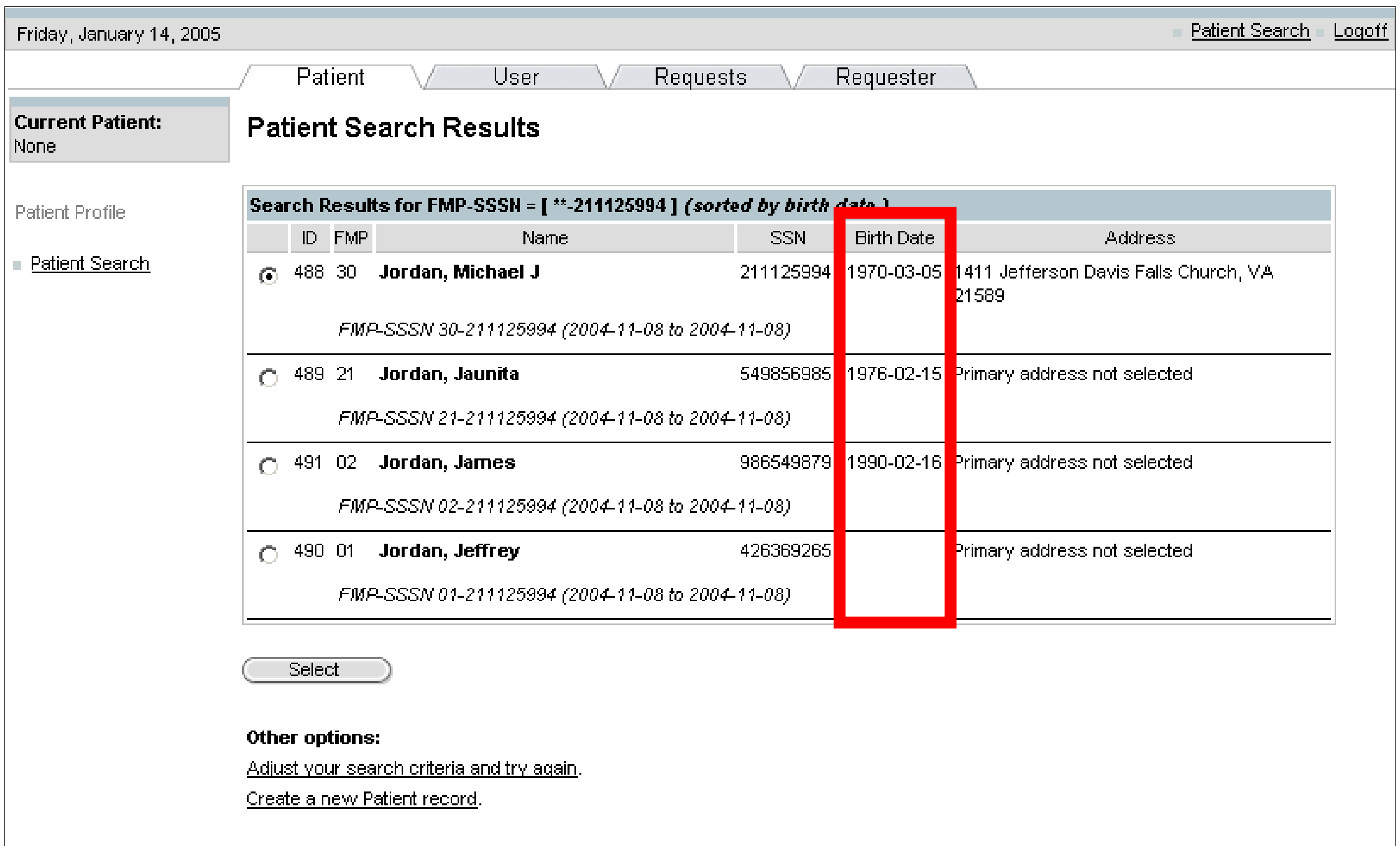
Partial Search (No FMP) (1 of 4)

1. Type in an asterisk in the FMP text box followed by the Sponsor's SSN
2. Click on the Search button



Partial Search (No FMP) (2 of 4)

3. The patient will appear followed by dependents sorted by Date of Birth (DOB) if present


Friday, January 14, 2005 — Patient Search | Logoff

Patient | User | Requests | Requester

Current Patient: None

Patient Profile

Patient Search

Patient Search Results

Search Results for FMP-SSSN = [**-211125994] *(sorted by birth date)*

	ID	FMP	Name	SSN	Birth Date	Address
(•)	488	30	**Jordan, Michael J**	211125994	1970-03-05	1411 Jefferson Davis Falls Church, VA 21589
			FMP-SSSN 30-211125994 (2004-11-08 to 2004-11-08)			
( )	489	21	**Jordan, Jaunita**	549856985	1976-02-15	Primary address not selected
			FMP-SSSN 21-211125994 (2004-11-08 to 2004-11-08)			
( )	491	02	**Jordan, James**	986549879	1990-02-16	Primary address not selected
			FMP-SSSN 02-211125994 (2004-11-08 to 2004-11-08)			
( )	490	01	**Jordan, Jeffrey**	426369265		Primary address not selected
			FMP-SSSN 01-211125994 (2004-11-08 to 2004-11-08)			

Select

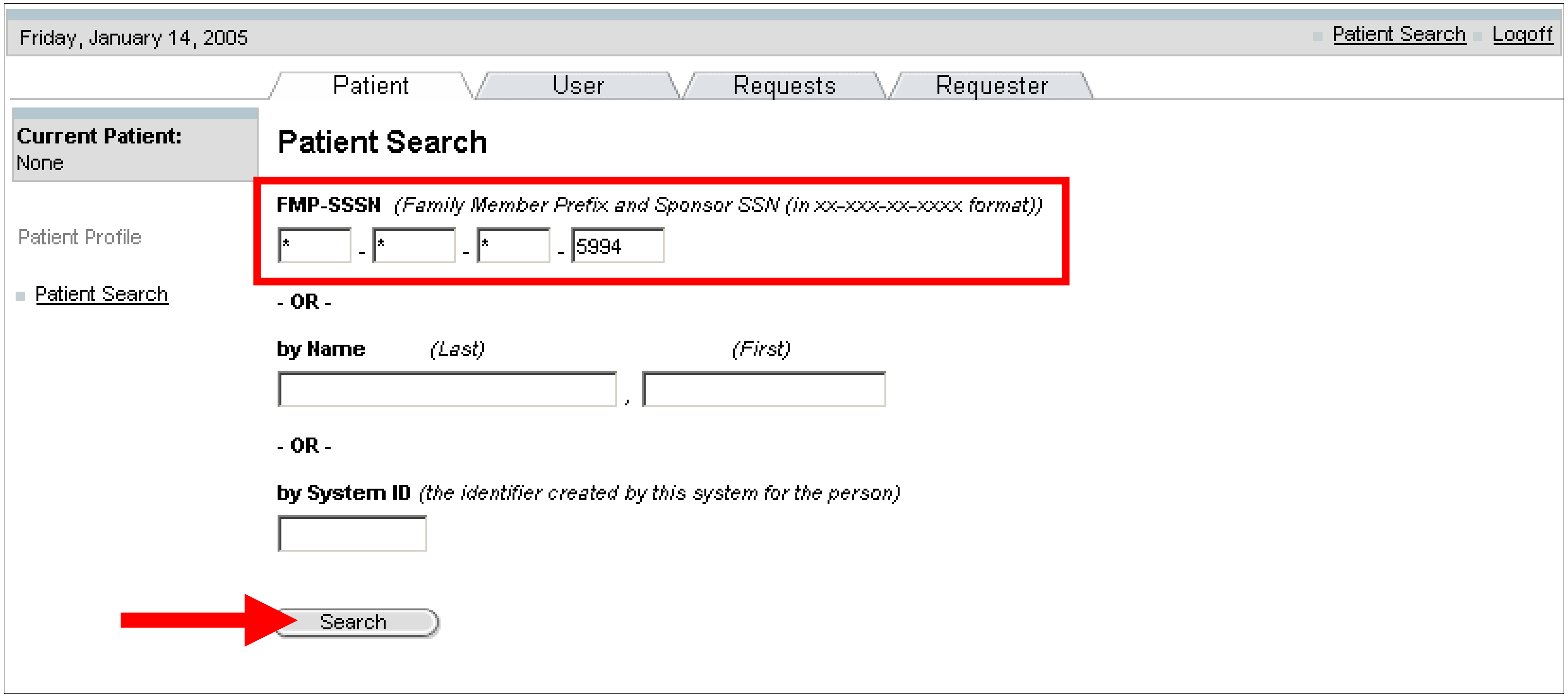
Other options:

Adjust your search criteria and try again.

Create a new Patient record.

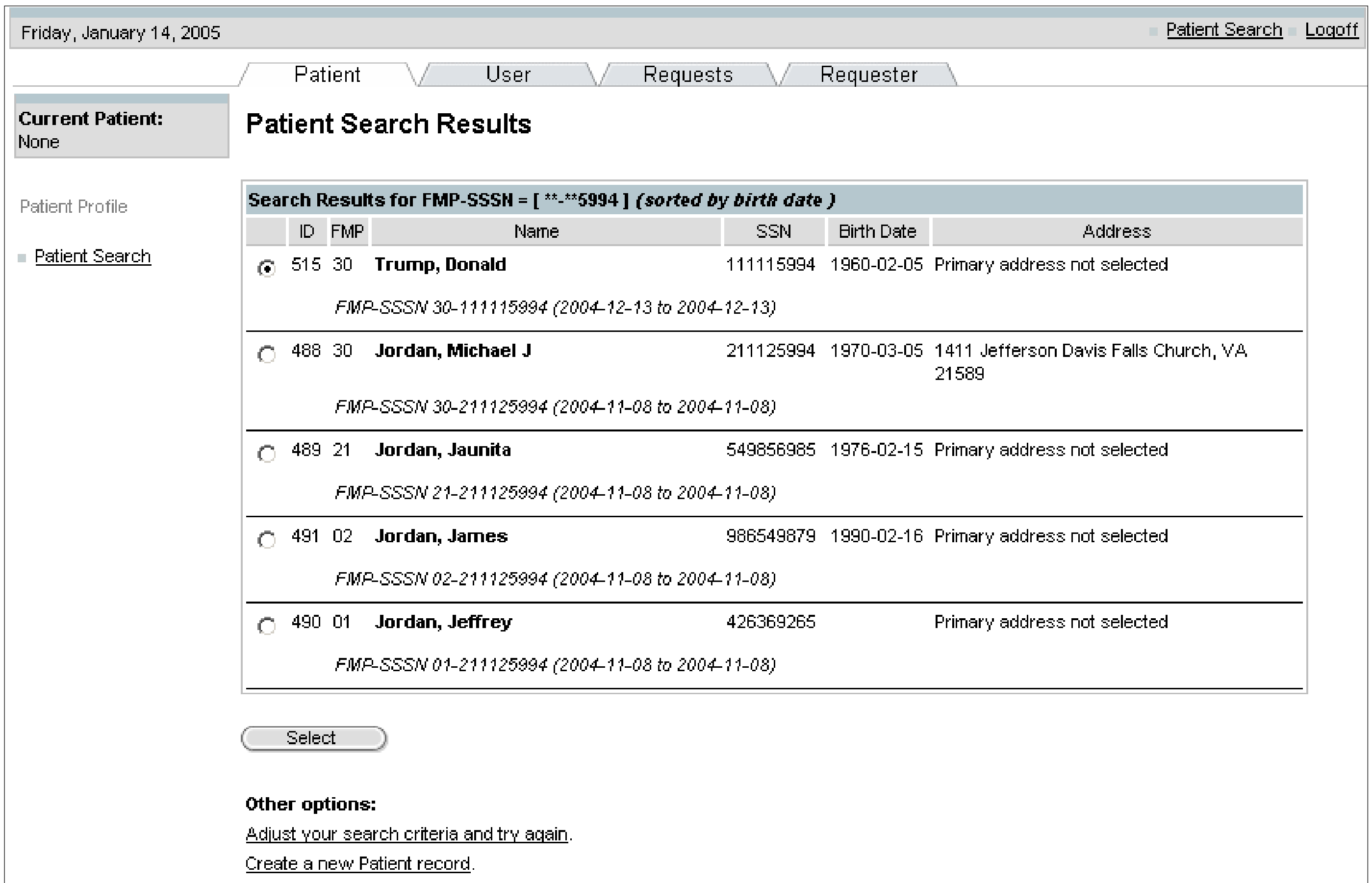
Partial Search (Last 4 digits) (3 of 4)

1. Type in an asterisk in the first three FMP-SSSN text fields followed by the last four digits of the Sponsor's SSN
2. Click on the Search button



Partial Search (Last 4 digits) (4of 4)

- The patients results screen will display all patients who have the last four digits of the SSN that was searched

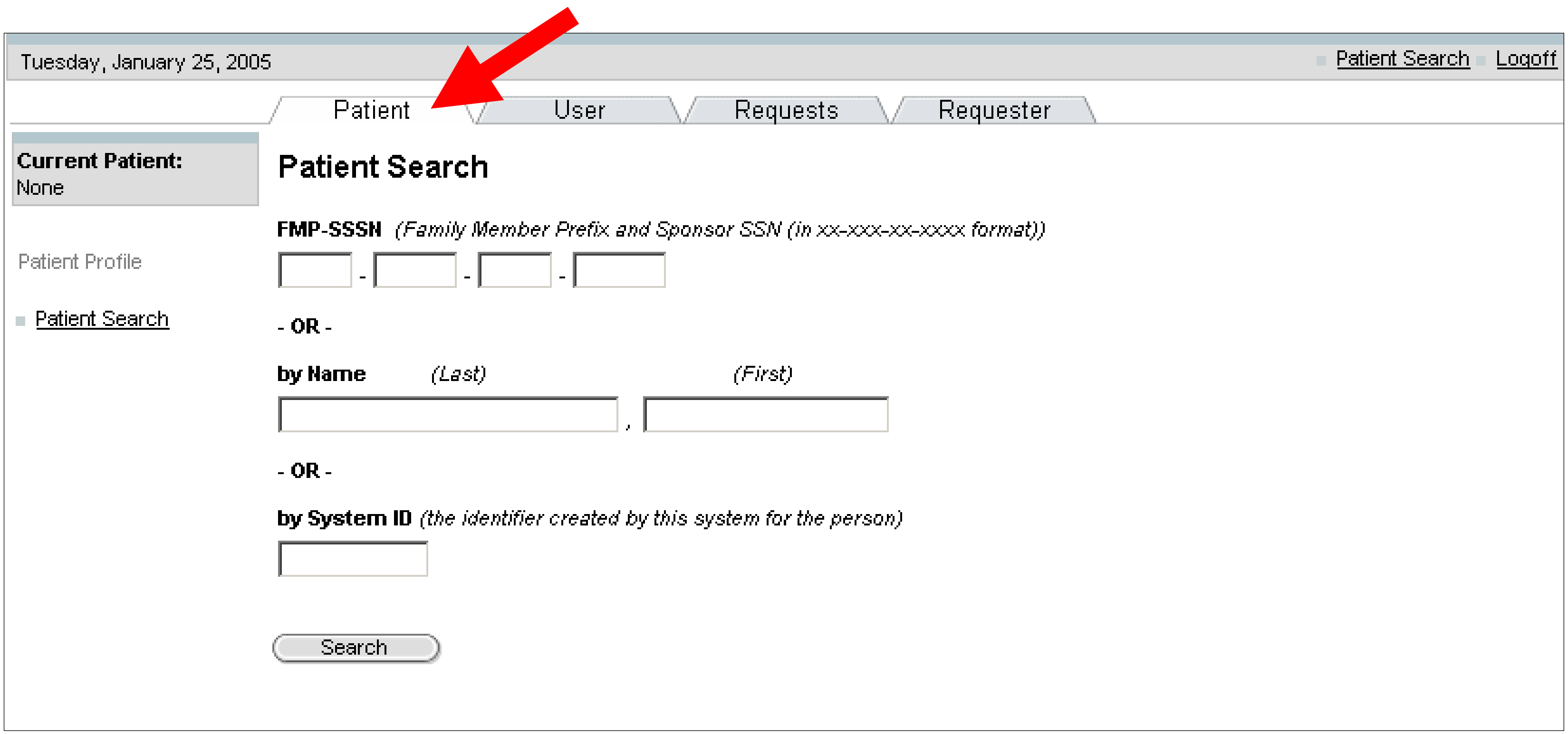


Add a Patient Record (1 of 6)

- If a patient record does not exist in the PHIMT database, then the user must add a patient record
- New patient records cannot be created without first searching the database

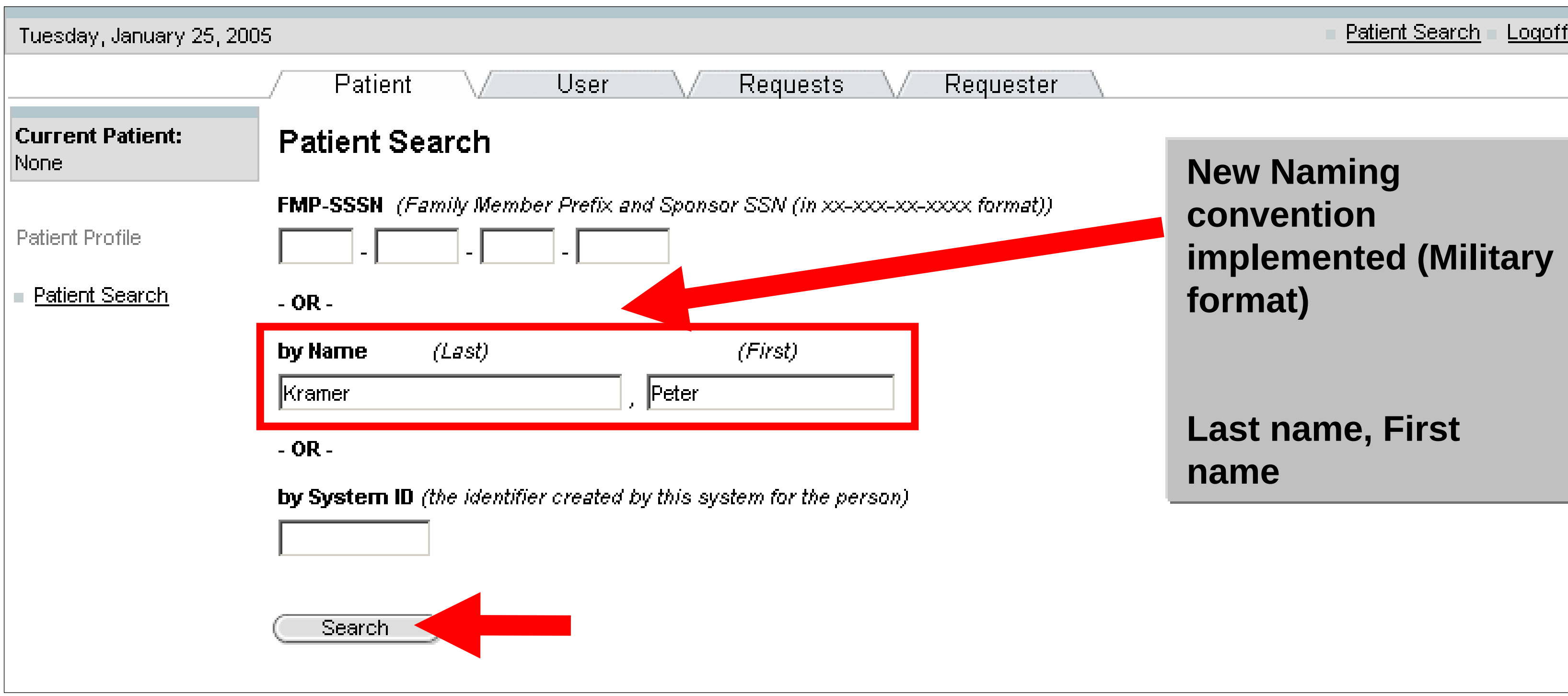
Add a Patient Record (2 of 6)

1. Select the Patient Tab



Add a Patient Record (3 of 6)

2. Type in the search criteria (patient’s name)
3. Click on the Search button

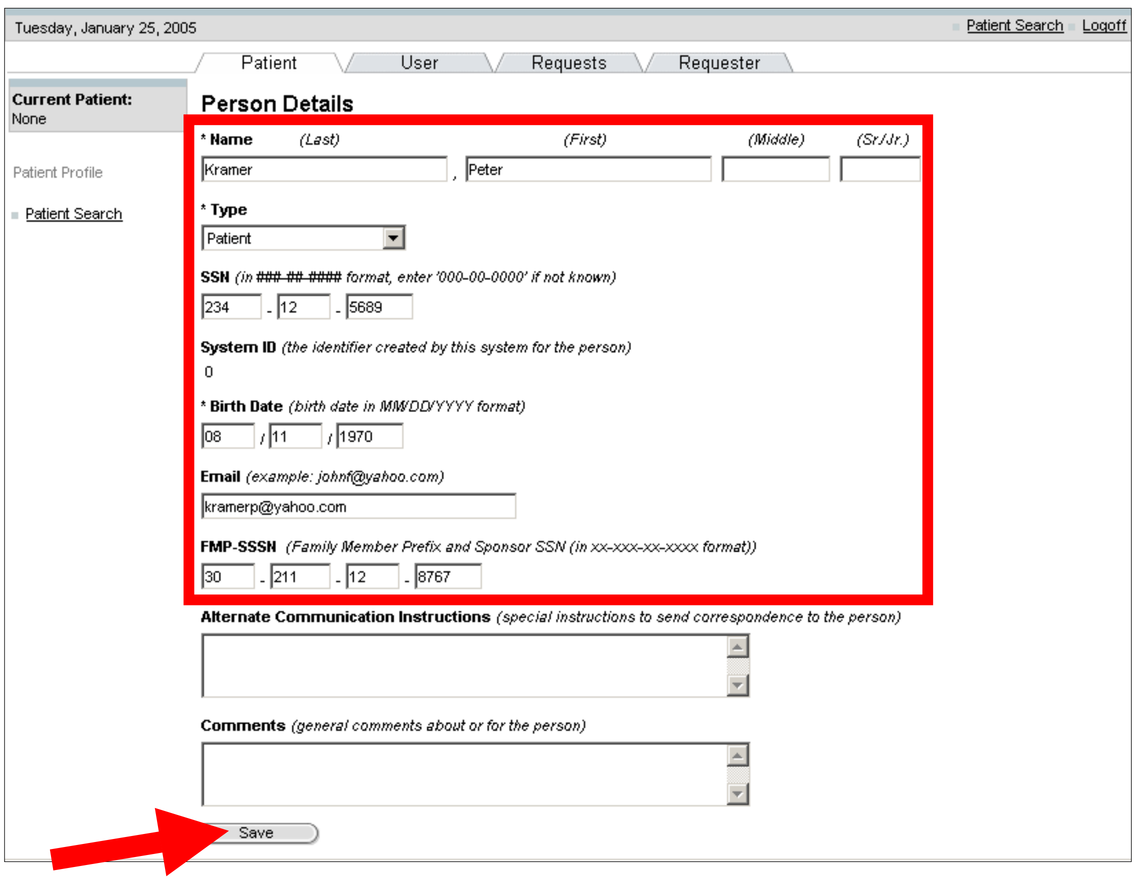


Add a Patient Record (4 of 6)

4. If no results matched your search, select the Create a New Patient Record hyperlink

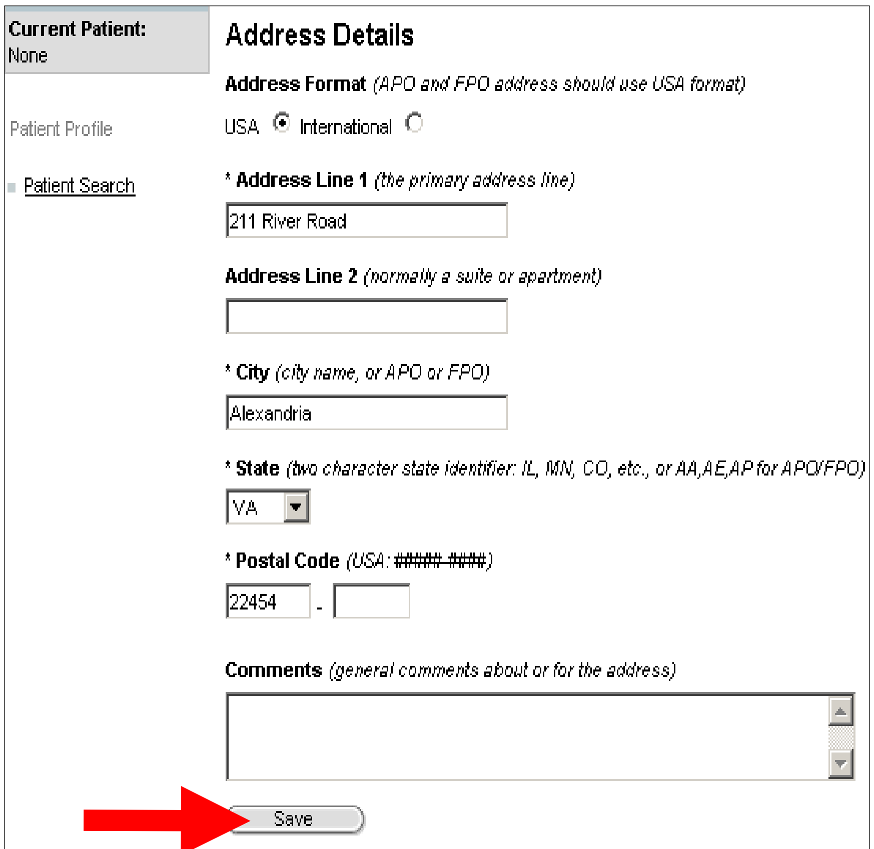
Add a Patient Record (5 of 6)

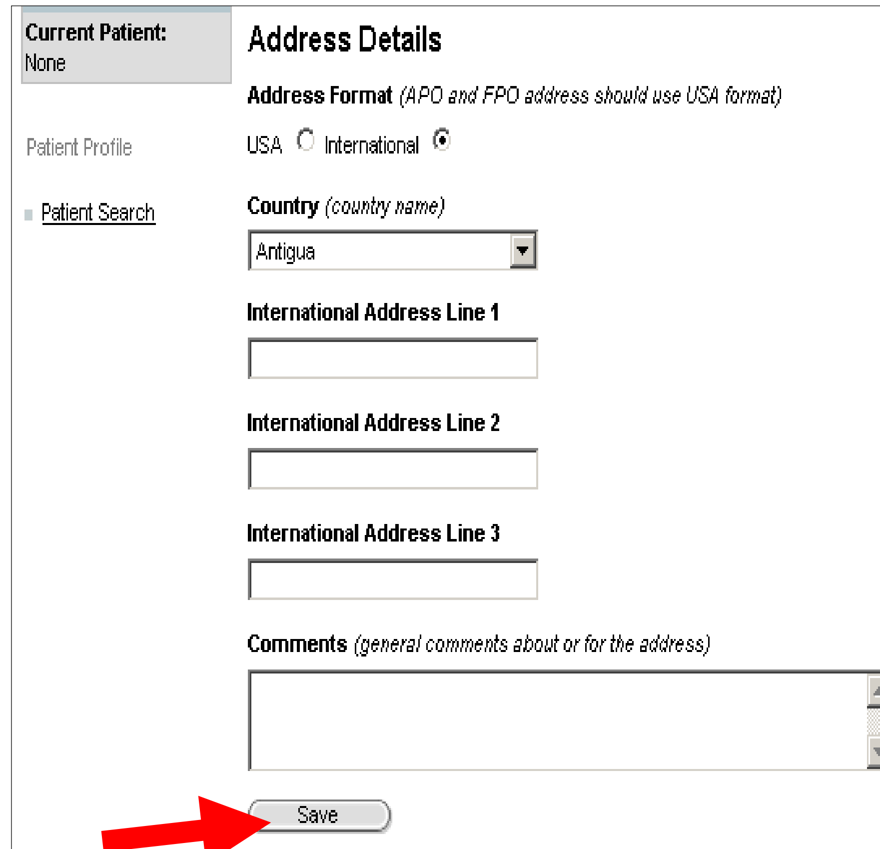
5. Enter Patient Information: (name, type, SSN, birth date, email, FMP-SSSN)
6. Click on the Save button



Add a Patient Record (6 of 6)

7. Enter Address Details: USA or International format
8. Click on the Save button





Create an Alternative Address (1 of 12)

- A covered entity shall permit individuals to request and shall accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations

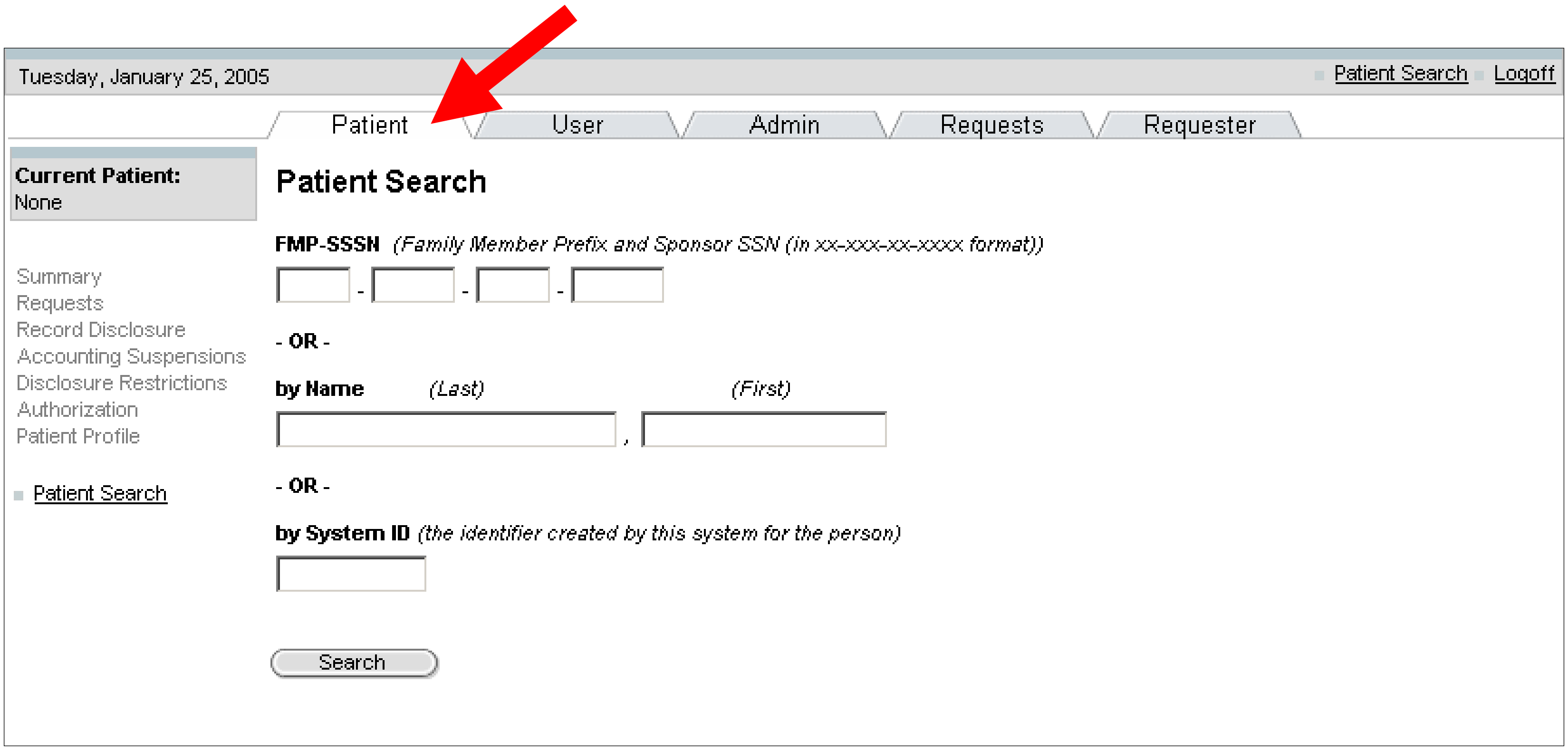
  -DoD 6025.18-R C10.2.2

  -164.522

- An alternative address can only be created by a Privacy Specialist

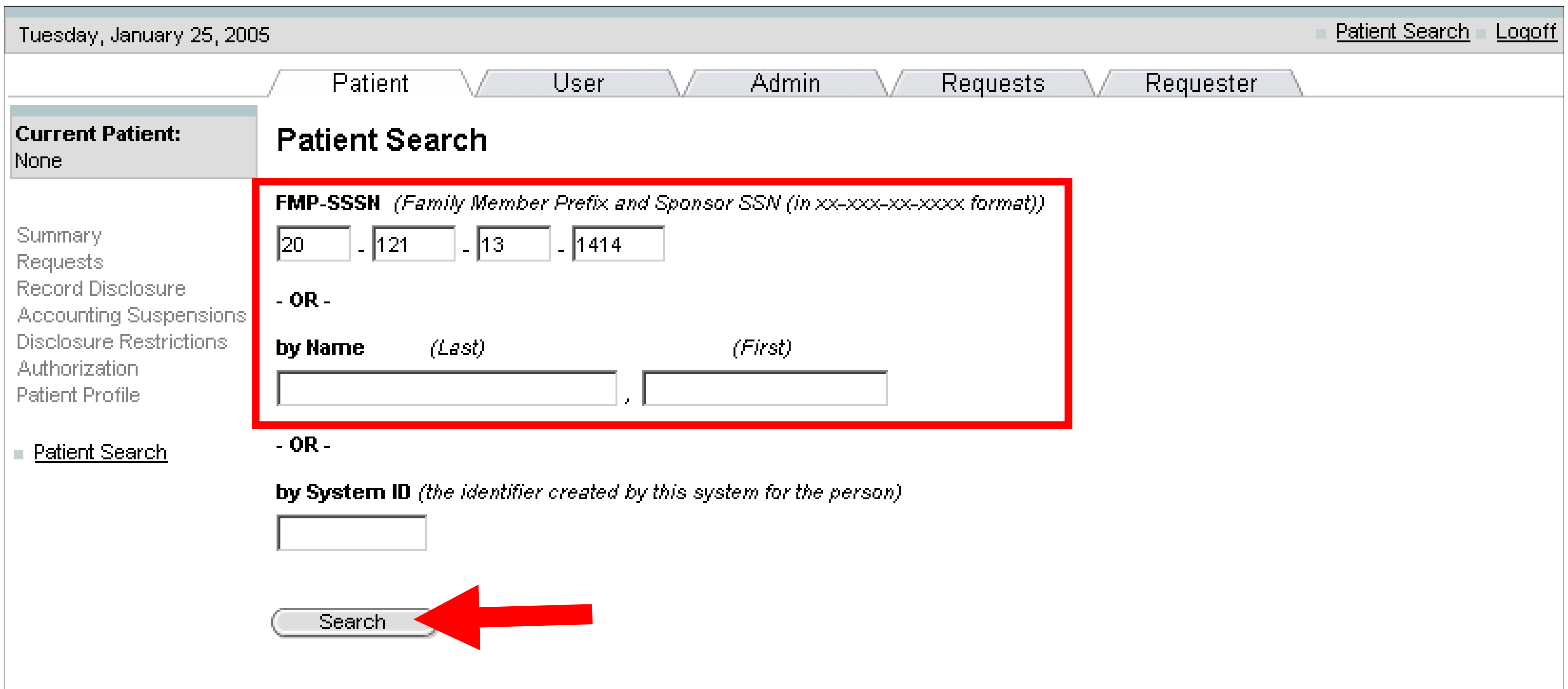
Create an Alternative Address (2 of 12)

1. Select the Patient Tab



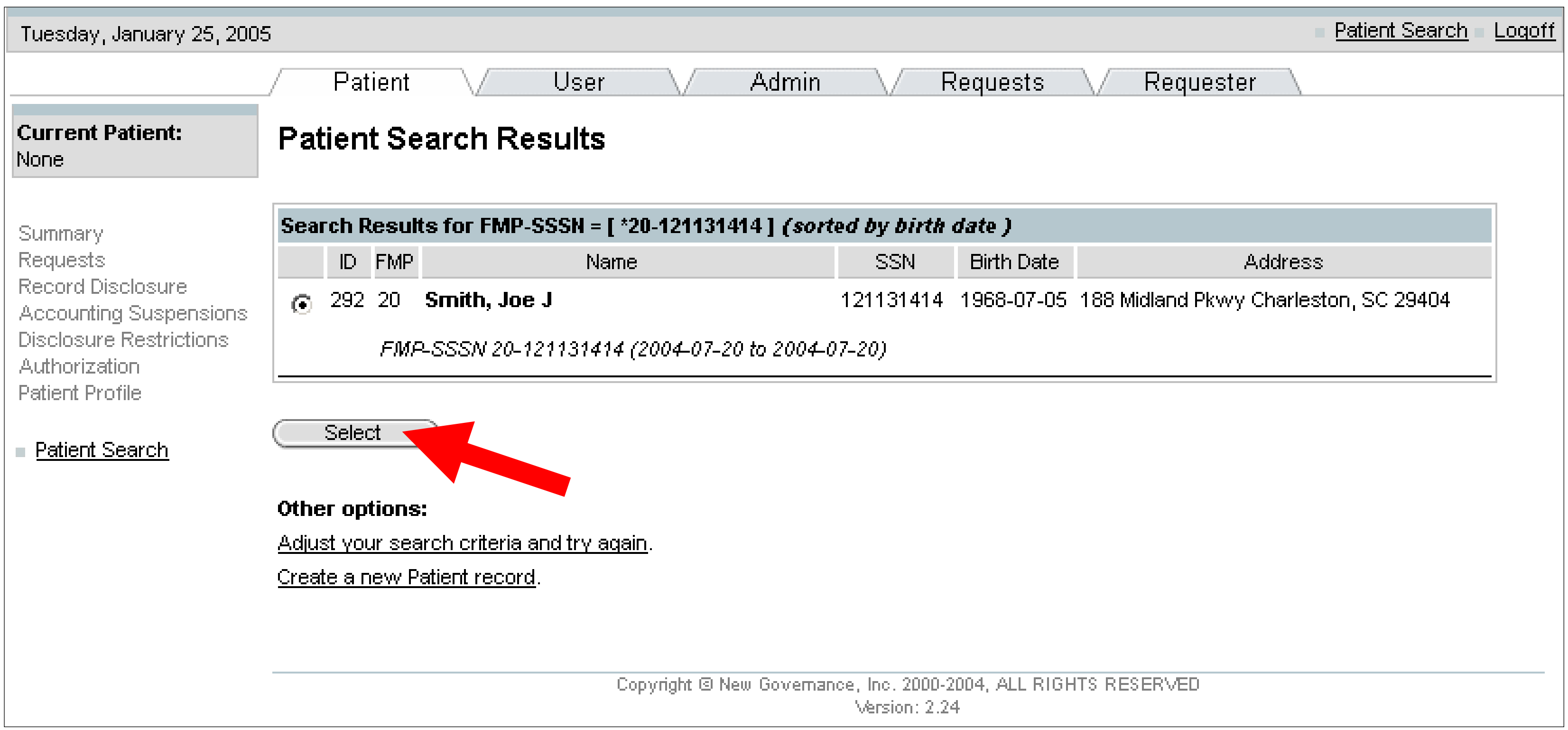
Create an Alternative Address (3 of 12)

2. Enter the patient search criteria
3. Click on the Search button



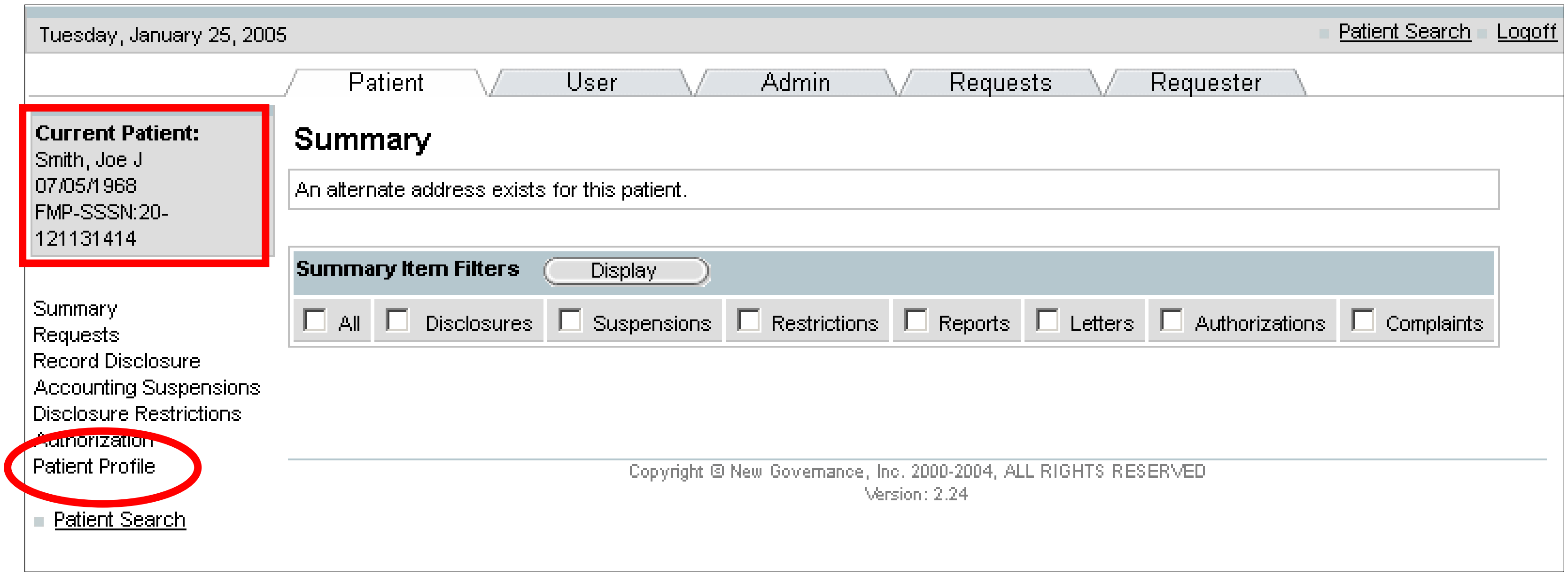
Create an Alternative Address (4 of 12)

4. Search Results will display
5. Select the patient



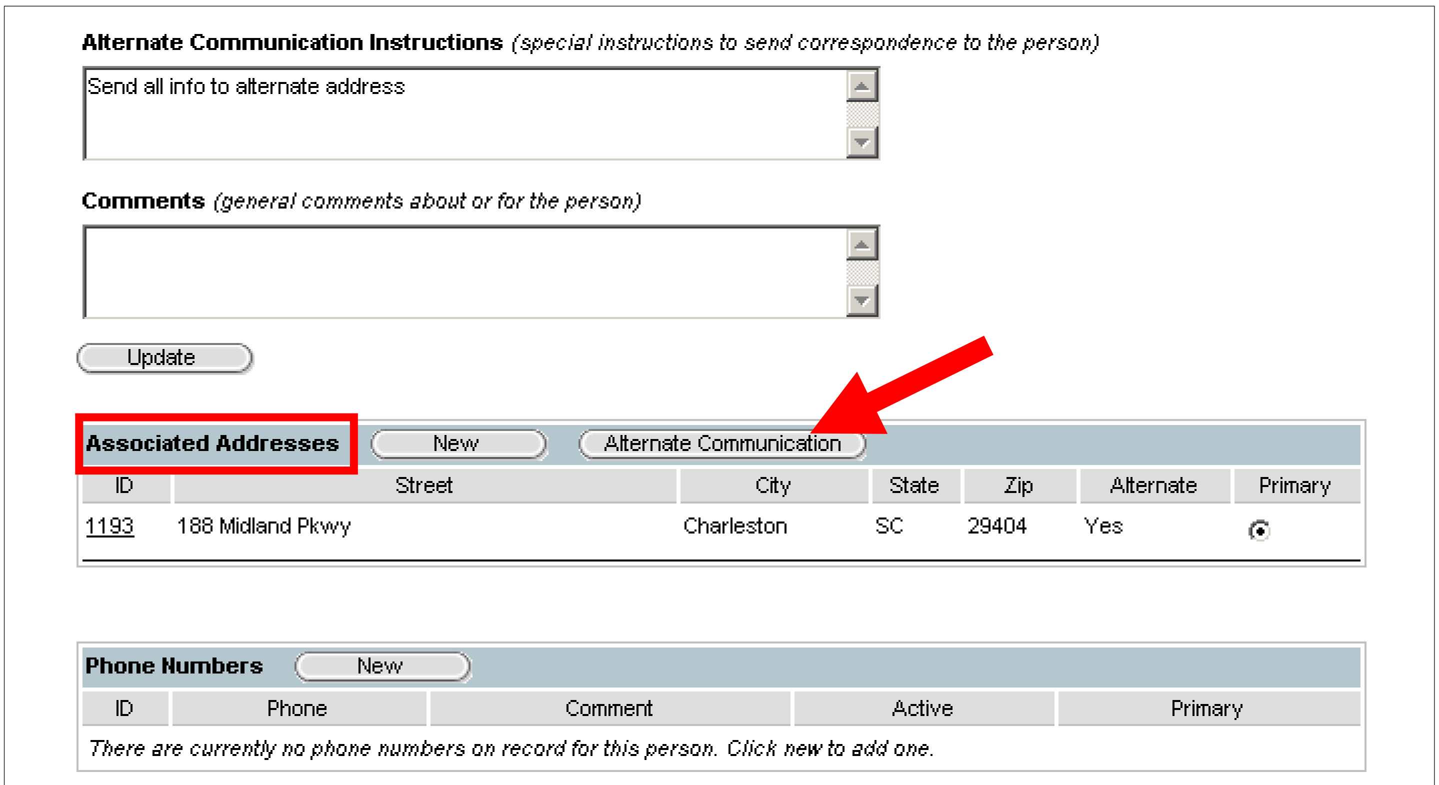
Create an Alternative Address (5 of 12)

6. Select the Patient Profile hyperlink



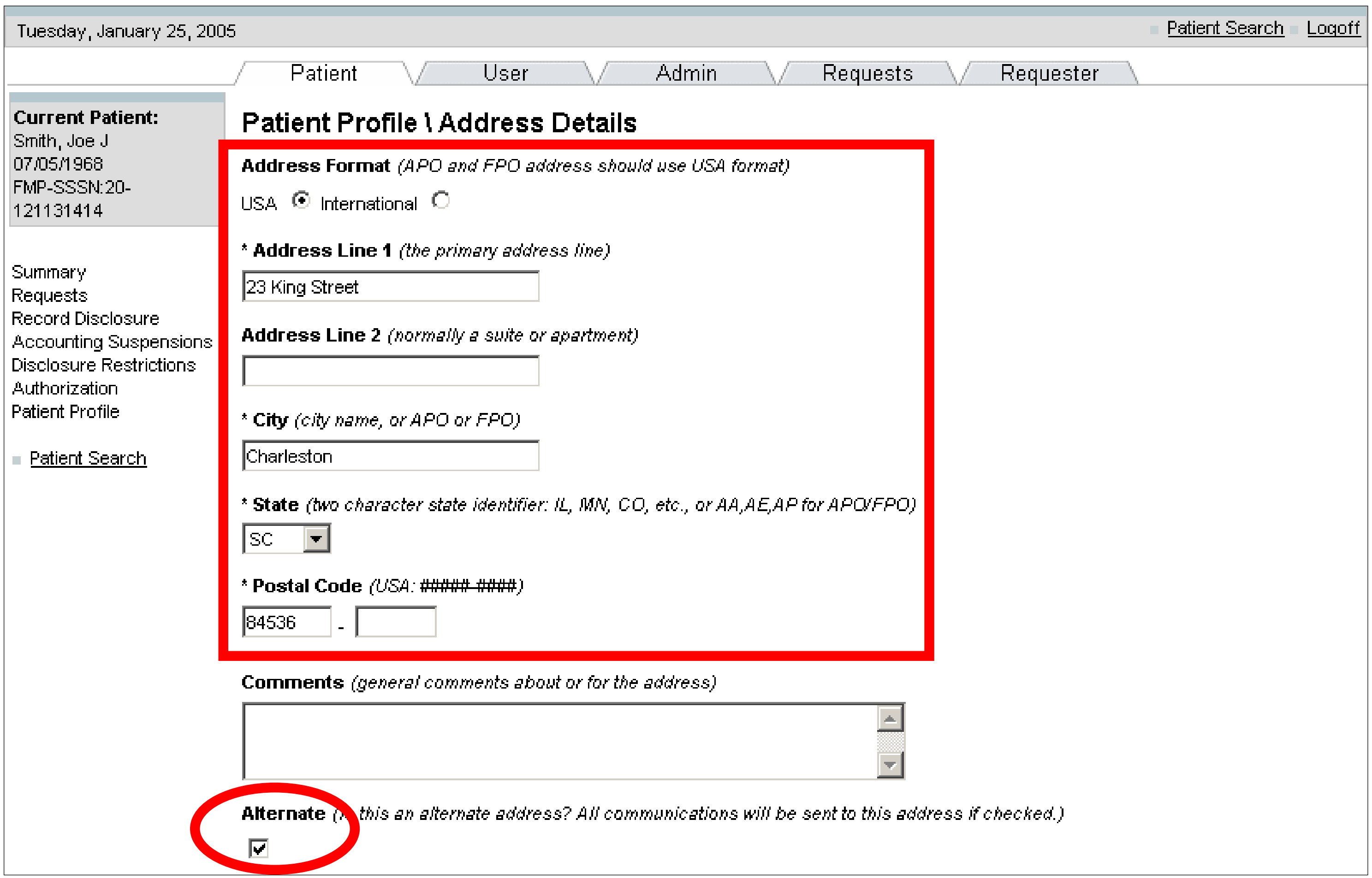
Create an Alternative Address (6 of 12)

7. Scroll down to the Associated Addresses box and click on the Alternative Communication button



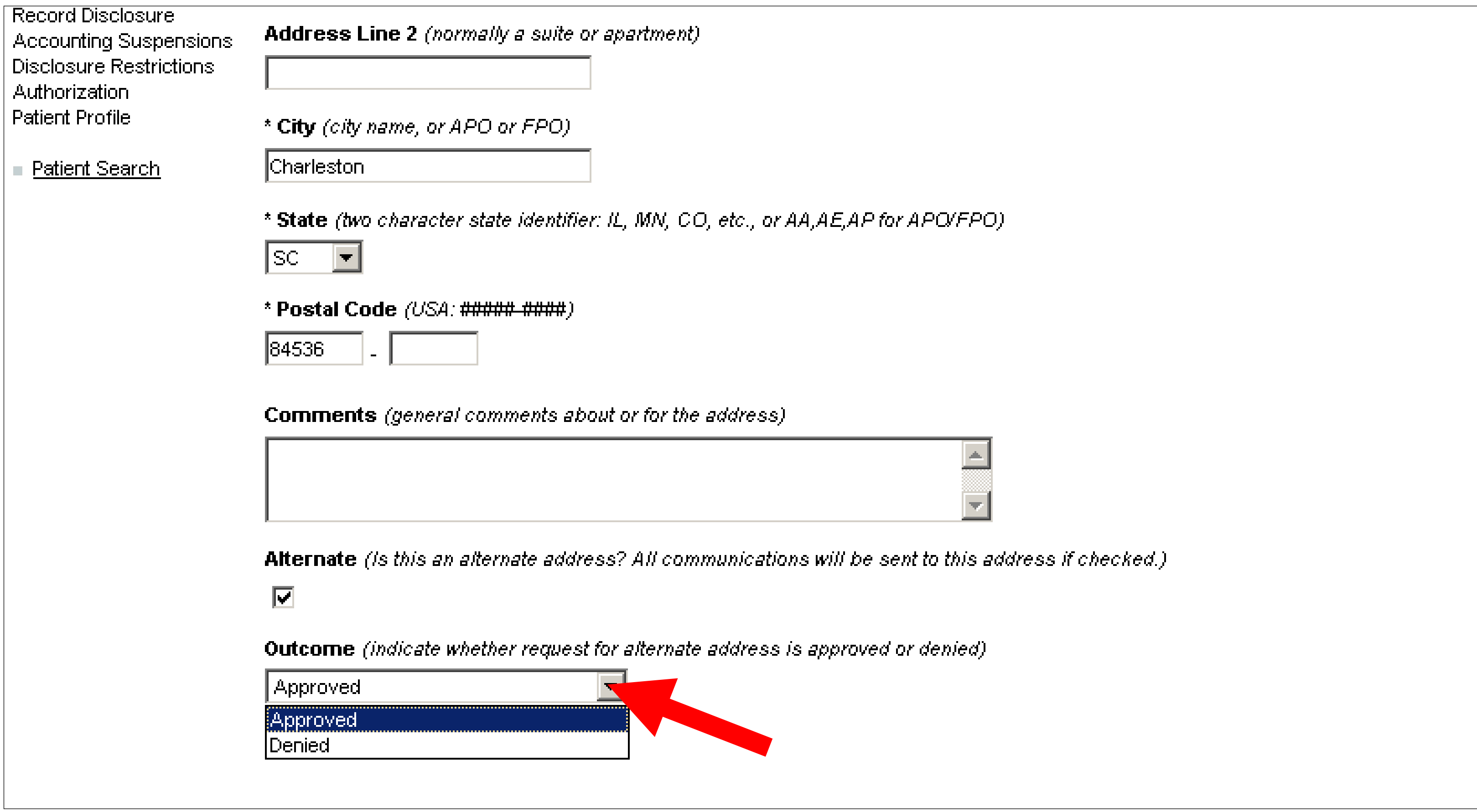
Create an Alternative Address (7 of 12)

8. Enter the Address Details: USA or International format
9. Put a check in the Alternate box



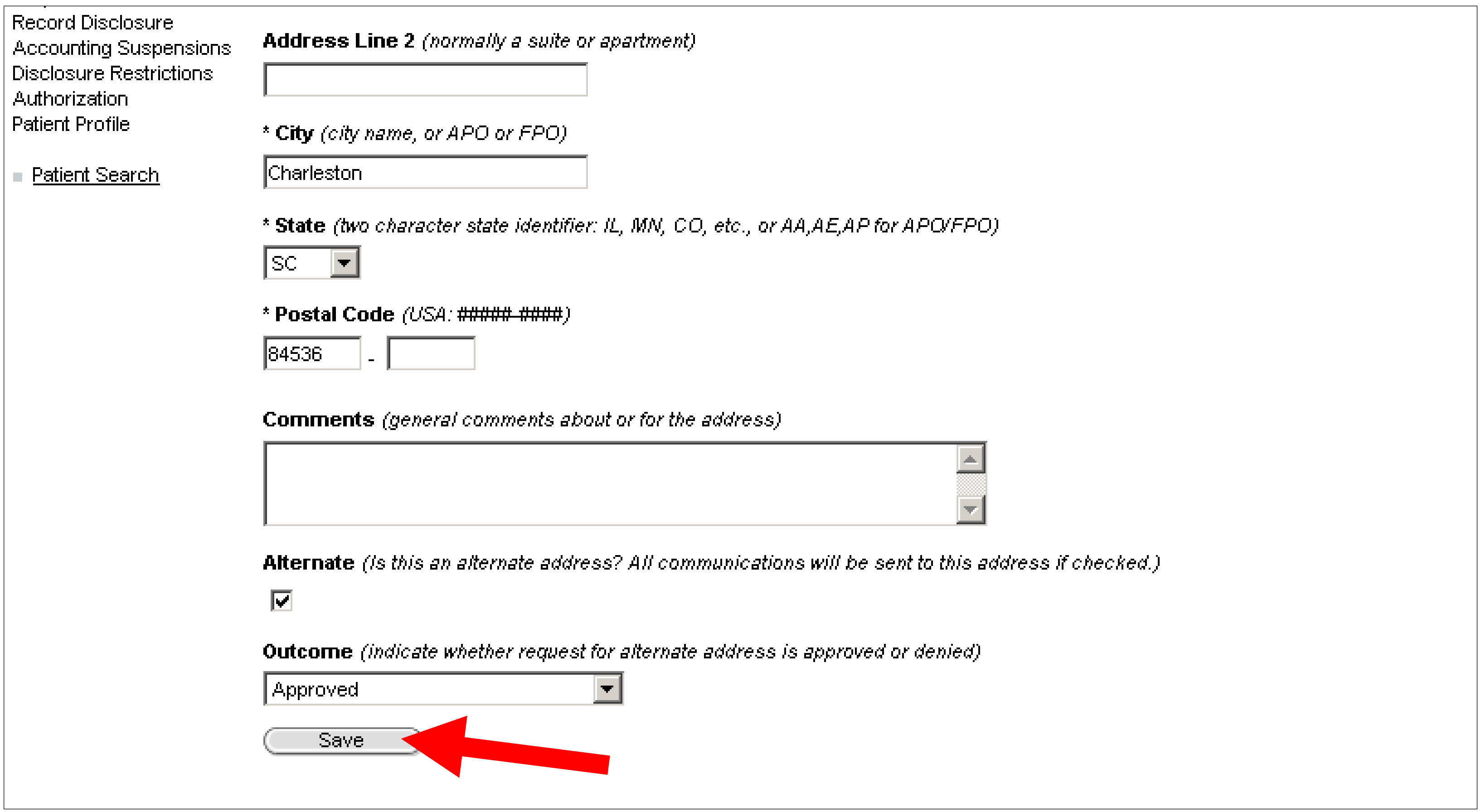
Create an Alternative Address (8 of 12)

10. Select Approved or Denied from the Outcome drop-down box



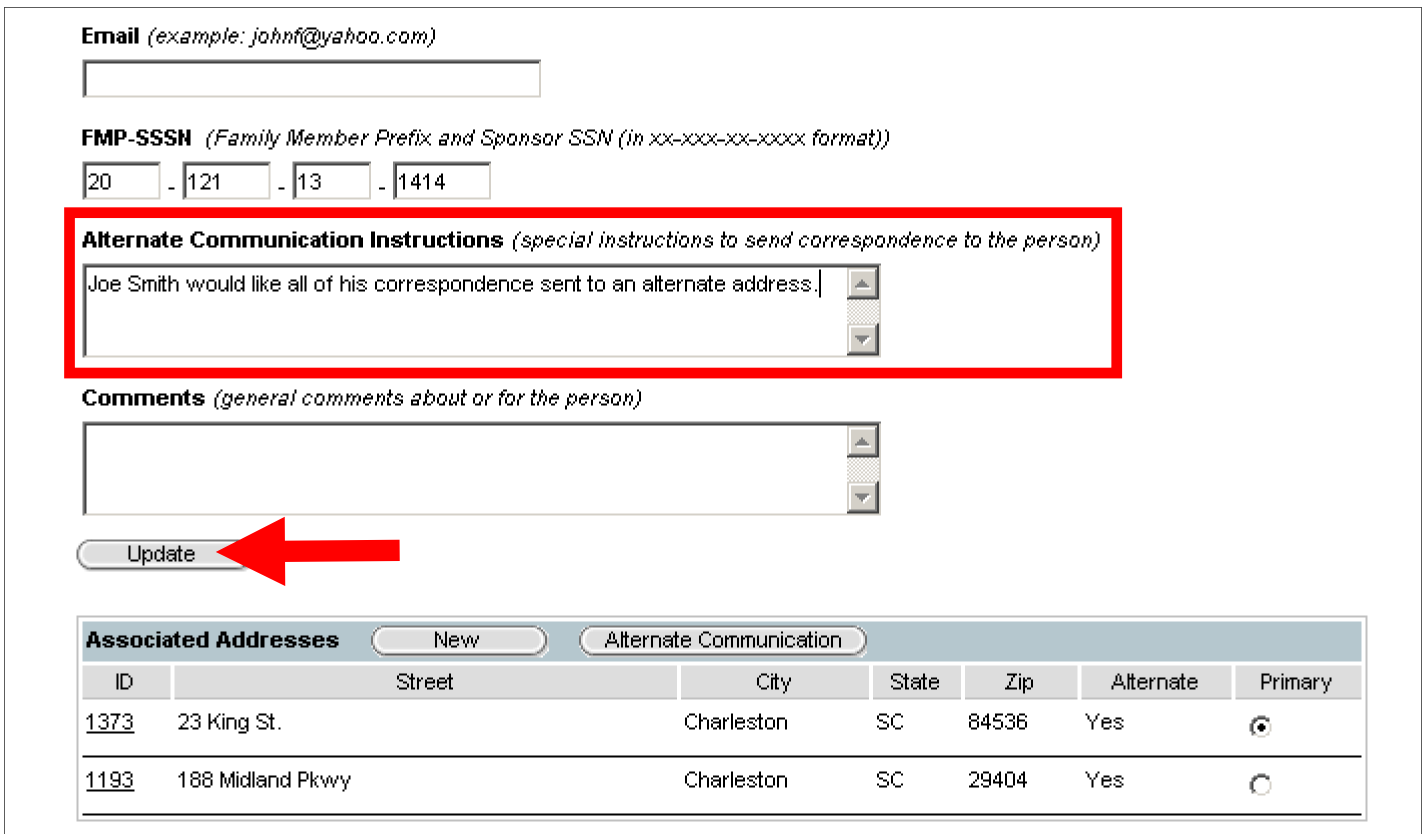
Create an Alternative Address (9 of 12)

11. Once the outcome is selected, click on the Save button



Create an Alternative Address (10 of 12)

12. Enter an appropriate comment in the Alternate Communication Instructions text box
13. Click on the Update button



Email *(example: johnf@yahoo.com)*

FMP-SSSN *(Family Member Prefix and Sponsor SSN (in xx-xxx-xx-xxxx format))*

20 - 121 - 13 - 1414

Alternate Communication Instructions *(special instructions to send correspondence to the person)*

Joe Smith would like all of his correspondence sent to an alternate address.

Comments *(general comments about or for the person)*

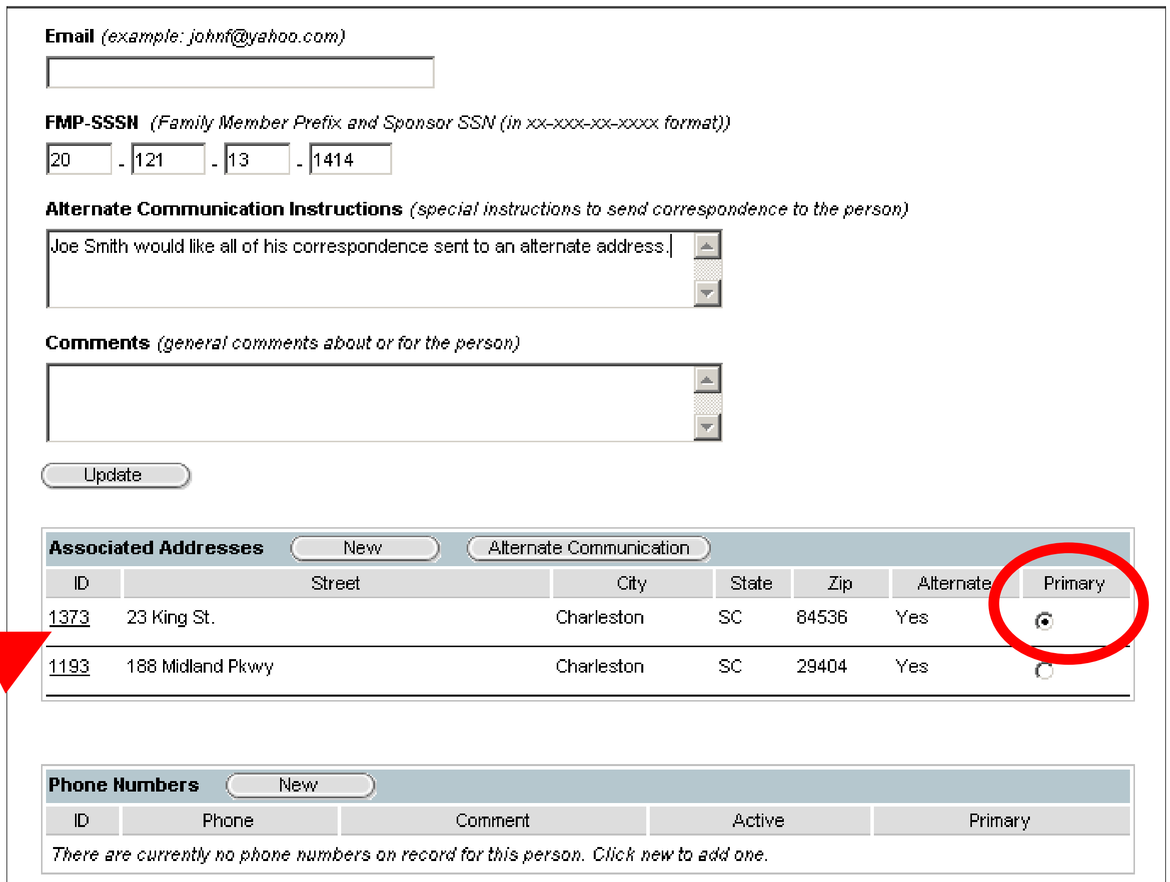
Update

Associated Addresses New Alternate Communication

ID	Street	City	State	Zip	Alternate	Primary
1373	23 King St.	Charleston	SC	84536	Yes	◉
1193	188 Midland Pkwy	Charleston	SC	29404	Yes	○

Create an Alternative Address (11 of 12)

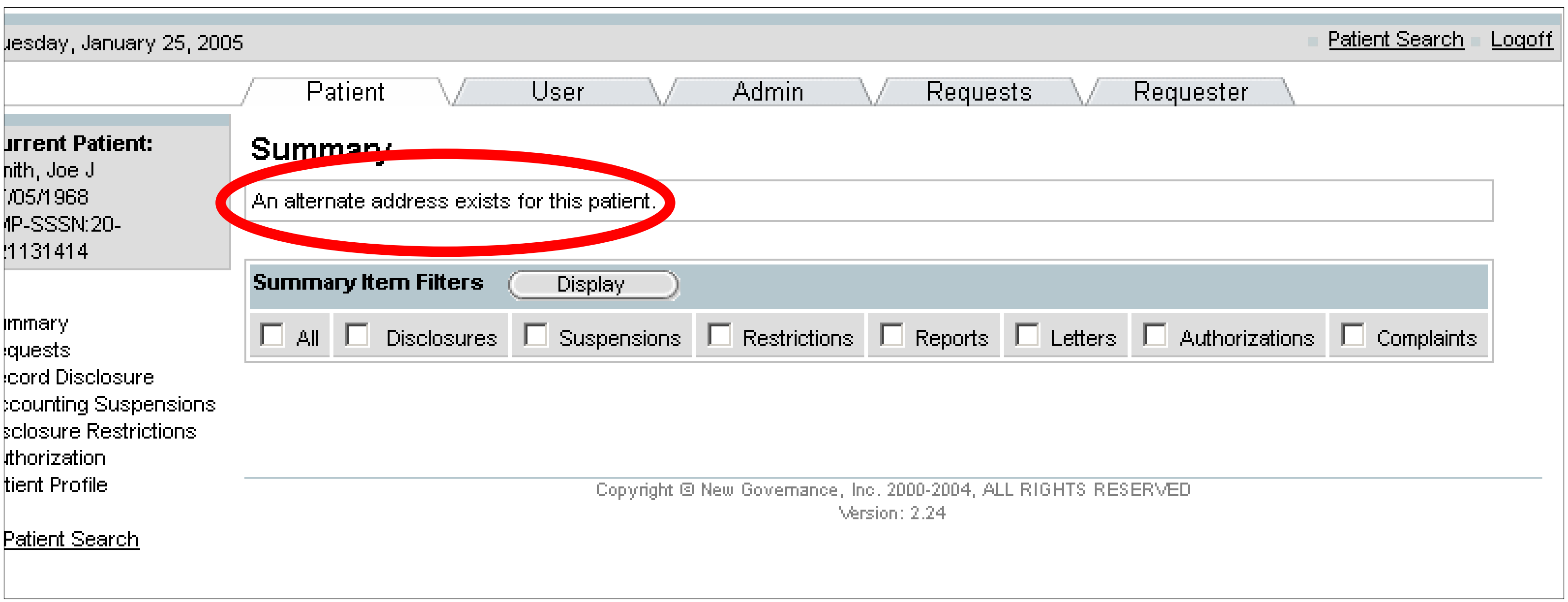
14. Scroll to the bottom of the Patient Profile screen to view the added alternative address



Patient Records

Create an Alternative Address (12 of 12)

- After an alternative address has been recorded, a note will appear on the Patient Summary Screen

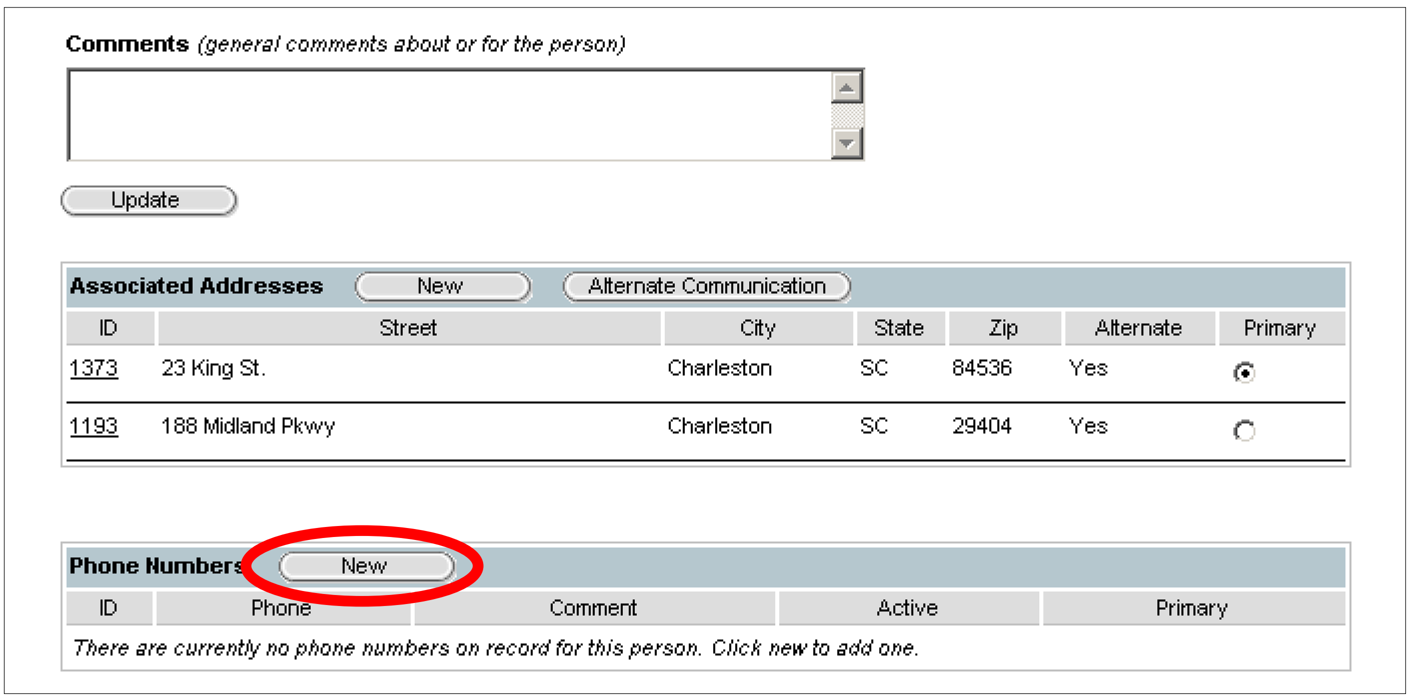


Create an Alternative Telephone Number (1 of 4)

- Individuals have the right to request an alternative telephone number for receiving communications related to their PHI
- An alternative telephone number can be created by Regular Users and Privacy Specialists

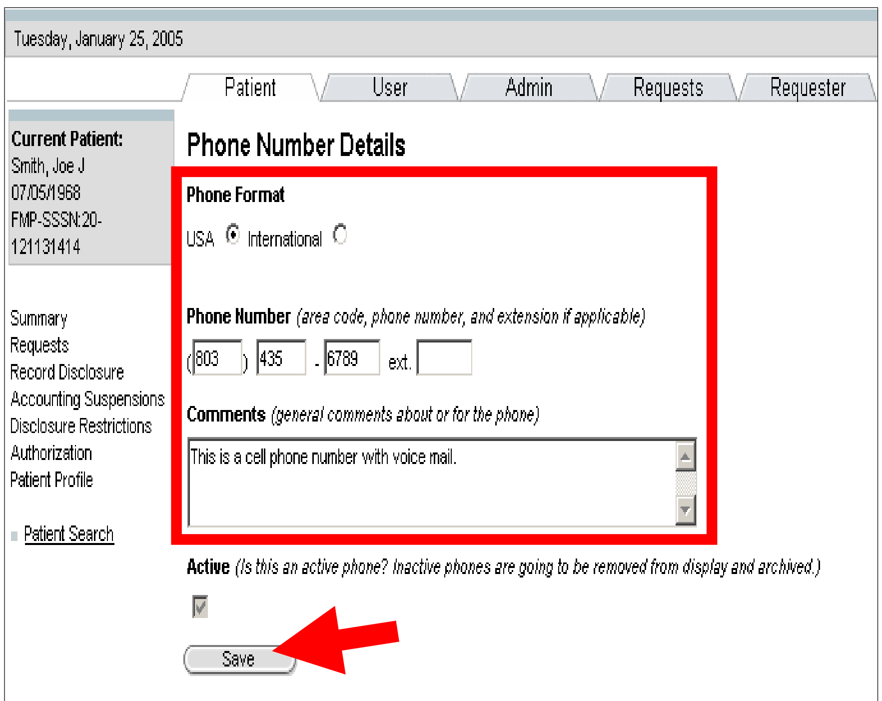
Create an Alternative Telephone Number (2 of 4)

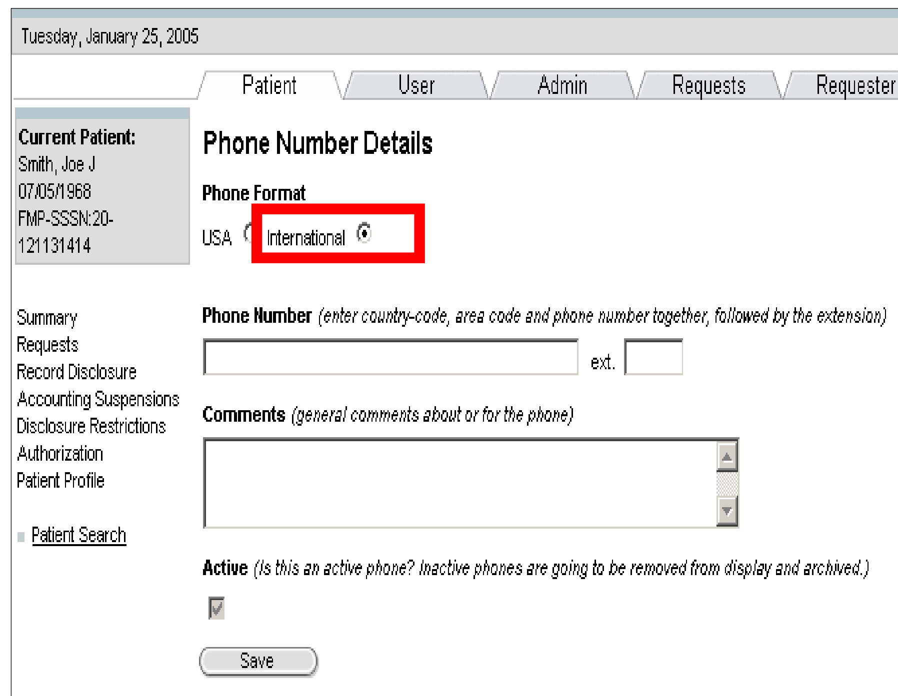
1. Scroll to the bottom of the Patient Details screen
2. Click on the New button next to Phone Numbers



Create an Alternative Telephone Number (3 of 4)

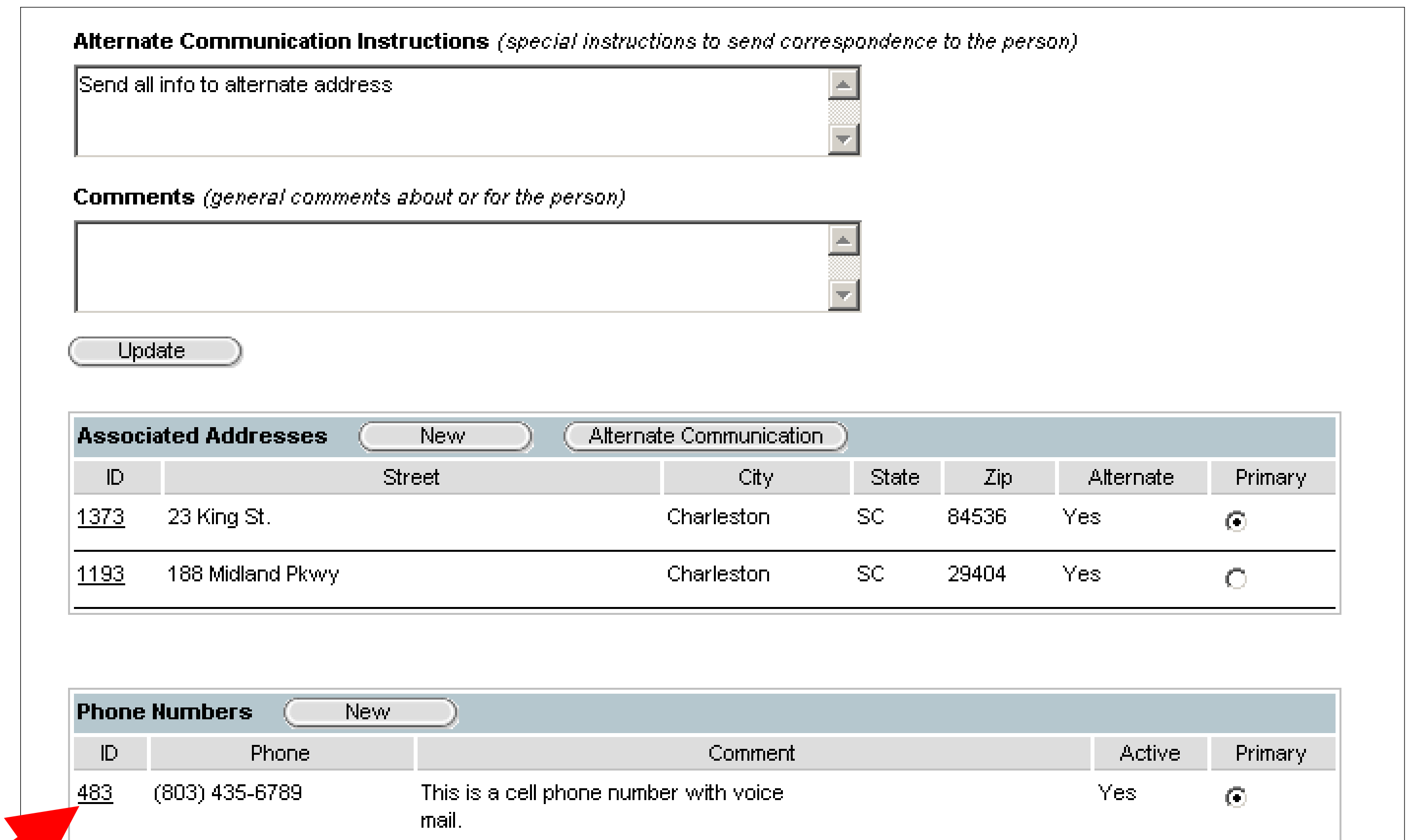
3. The Phone Number Details screen will display (choose USA or International format)
4. Type in the phone number and enter any comments
5. Click on the Save button





Create an Alternative Telephone Number (4 of 4)

6. The phone number you added will appear on the Patient Details screen



Alternate Communication Instructions *(special instructions to send correspondence to the person)*

Send all info to alternate address

Comments *(general comments about or for the person)*

Update

Associated Addresses New Alternate Communication

ID	Street	City	State	Zip	Alternate	Primary
1373	23 King St.	Charleston	SC	84536	Yes	◉
1193	188 Midland Pkwy	Charleston	SC	29404	Yes	○

Phone Numbers New

ID	Phone	Comment	Active	Primary
483	(803) 435-6789	This is a cell phone number with voice mail.	Yes	◉

Summary

- You should now be able to:
  - Search for a patient record
  - Add a patient record
  - Create an alternative address
  - Create an alternative telephone number

Disclosures

Disclosures

Objectives

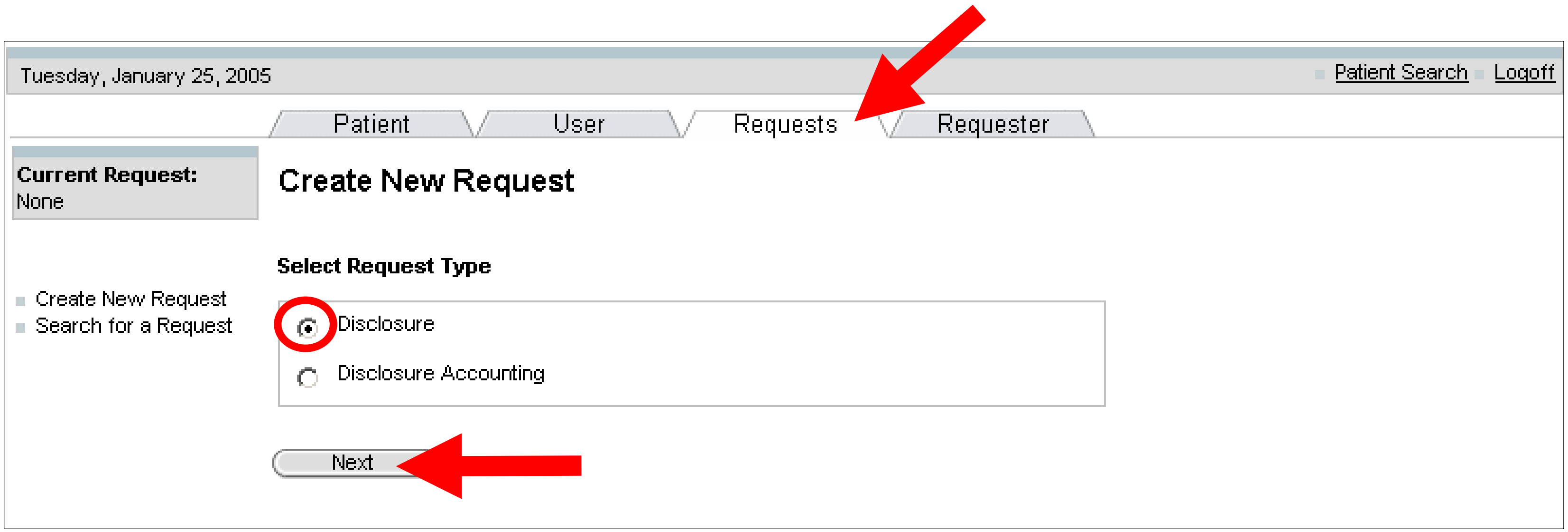
- Upon completion of this lesson, you will be able to:
  - Record a request for disclosure as a Regular User
    - Regular Users can now update the Patient’s address in the middle of a disclosure request
  - Record a disclosure as a Privacy Specialist
  - Approve/deny a disclosure
  - Amend a disclosure

Recording a Request for Disclosure (1 of 12)

- Individuals have the right to an accounting of disclosures
- DoD 6025.18-R requires us to record specific information
- Chapter 13 pertains to the Accounting of Disclosures Policy
- Regular Users record requests for disclosures and route them to their Privacy Specialist for approval or denial

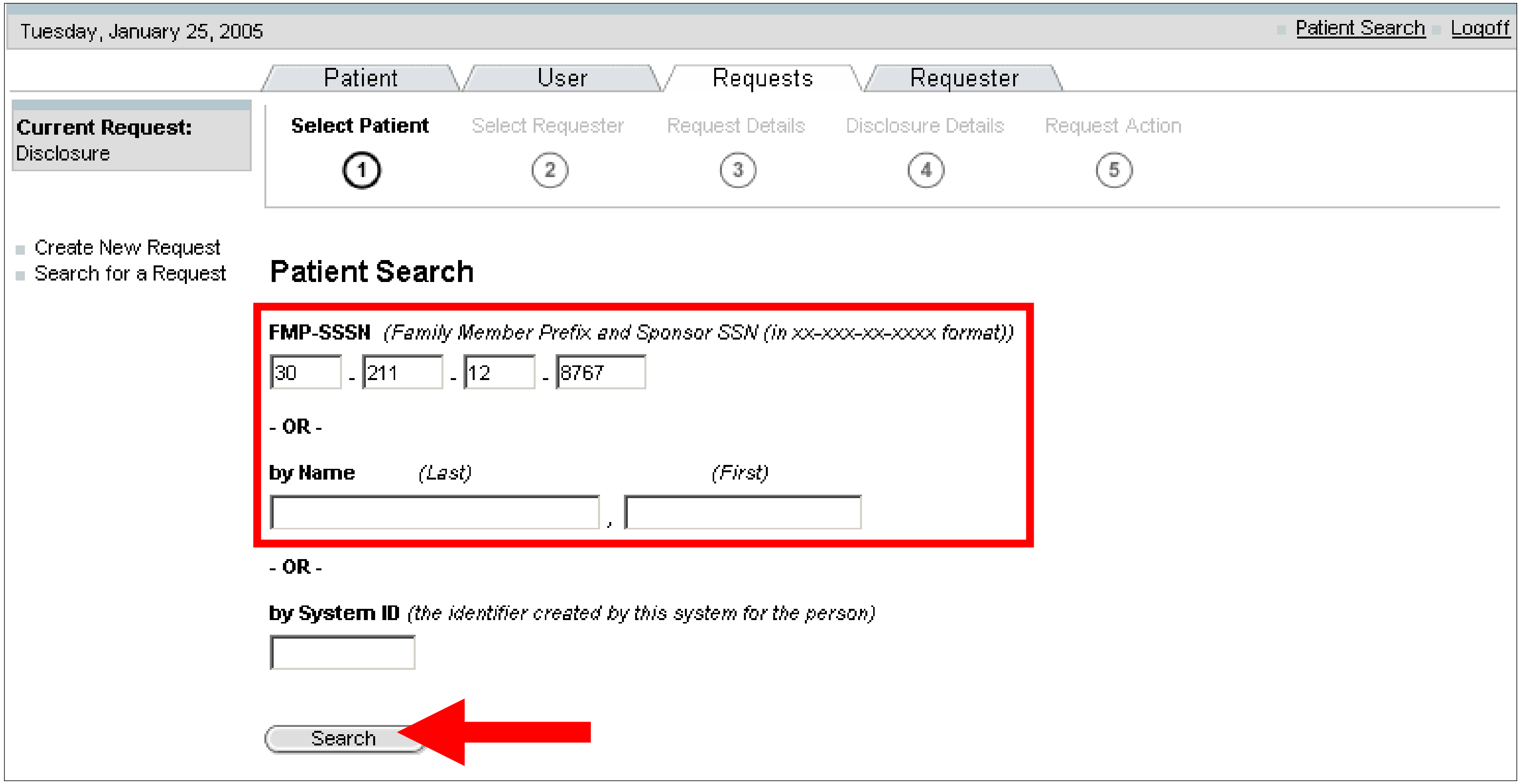
Recording a Request for Disclosure (2 of 12)

1. Select the Requests Tab
2. Click on the Disclosure Radio Button
3. Click on the Next button



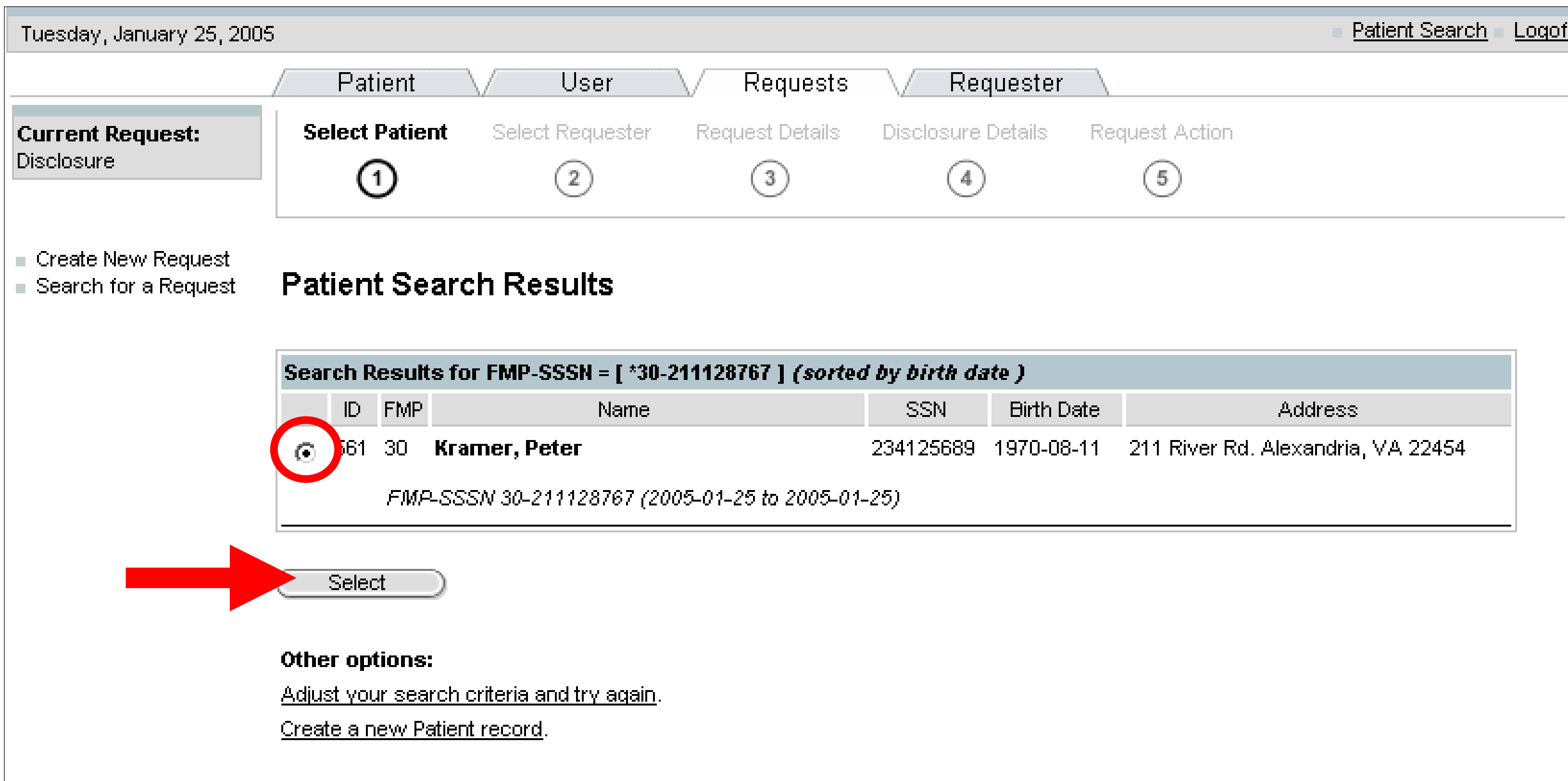
Recording a Request for Disclosure (3 of 12)

4. Enter patient search criteria
5. Click on the Search button



Recording a Request for Disclosure (4 of 12)

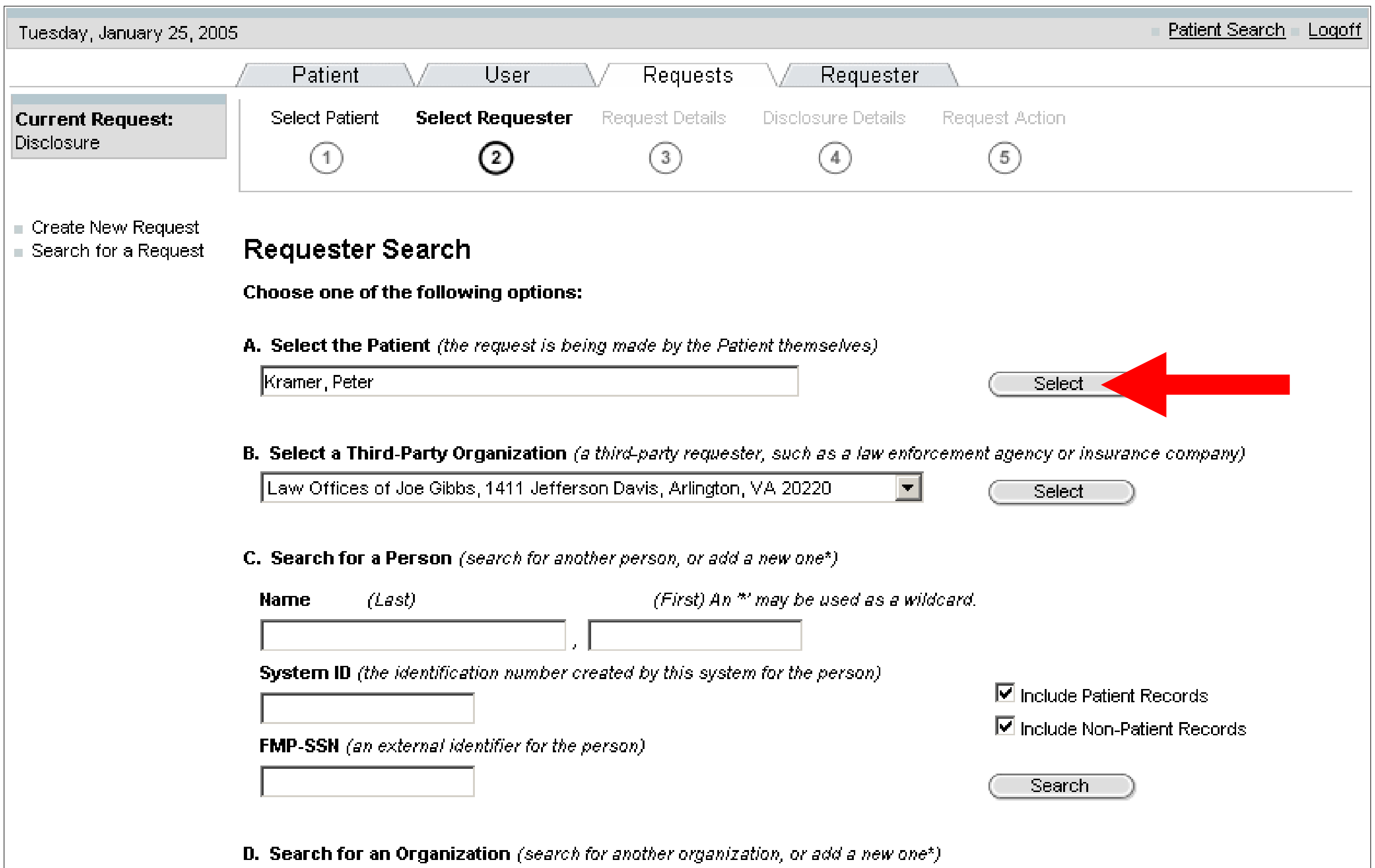
6. Select the radio button next to the patient's name
7. Click on the Select button



Recording a Request for Disclosure (5 of 12)

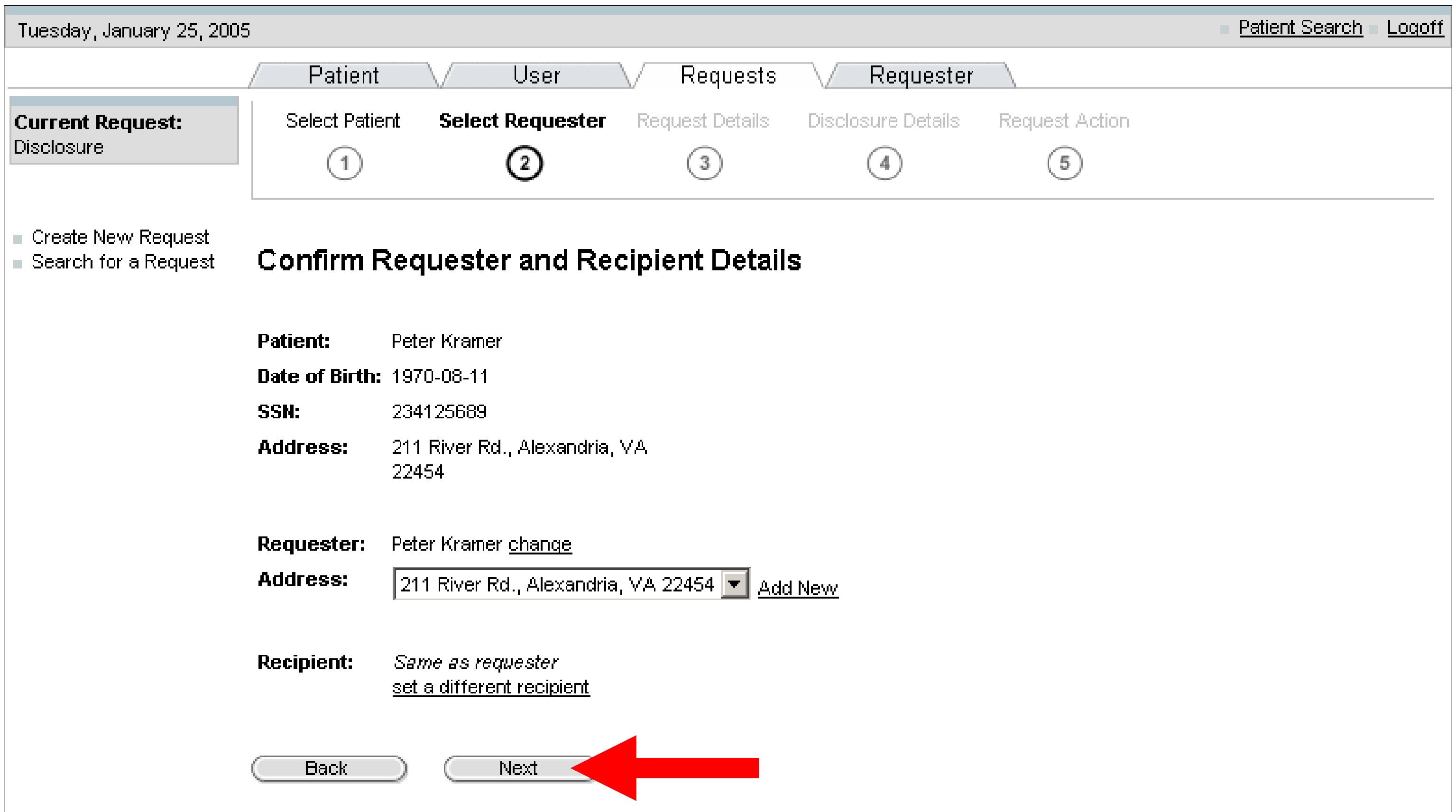
- If the request is being made by the patient themselves,

8. Click on the Select button next to the patient’s name



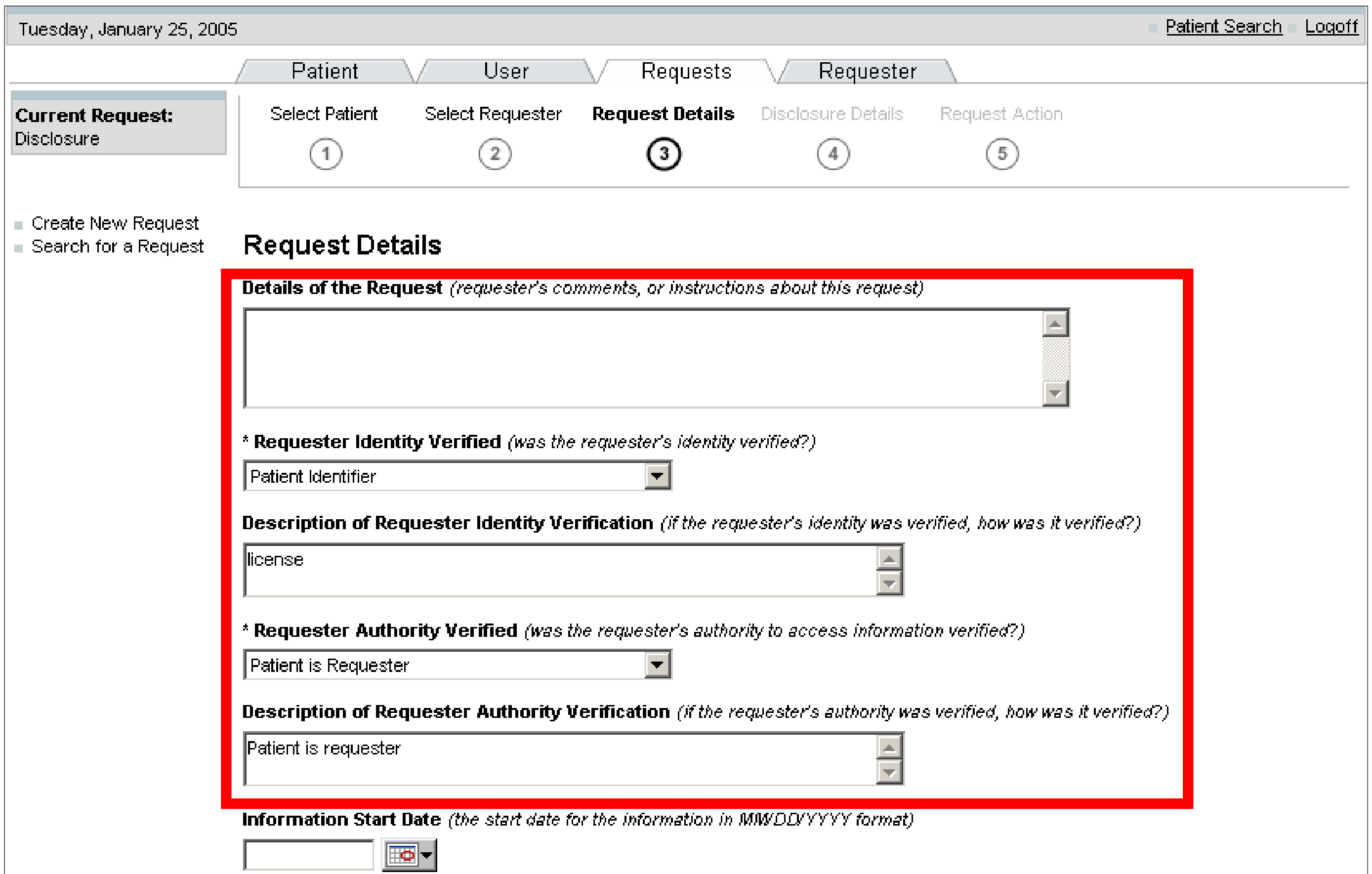
Recording a Request for Disclosure (6 of 12)

9. Confirm Requester and Recipient Details
10. Click on the Next button



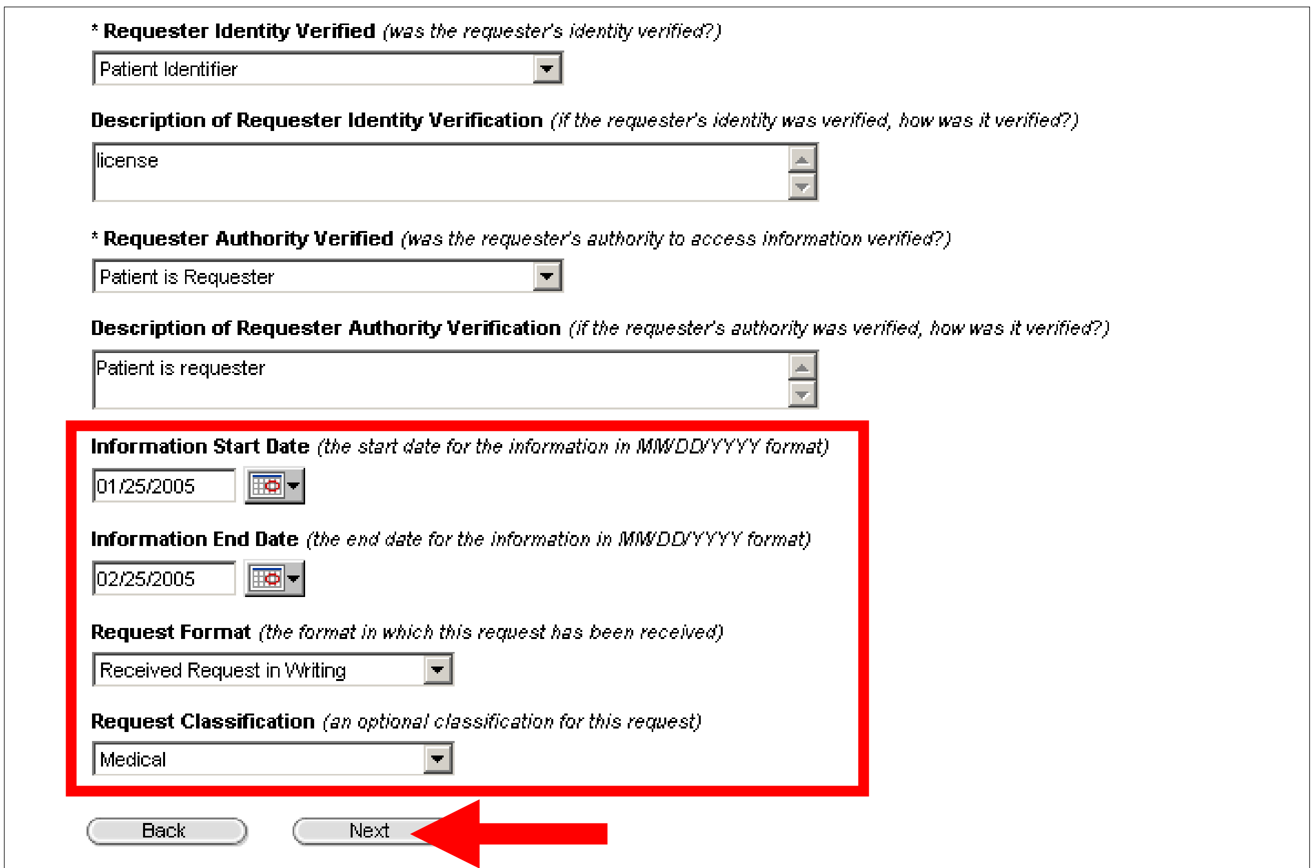
Recording a Request for Disclosure (7 of 12)

11. Enter in the Request Details: (details of the request, identity verification, and authority verification)



Recording a Request for Disclosure (8 of 12)

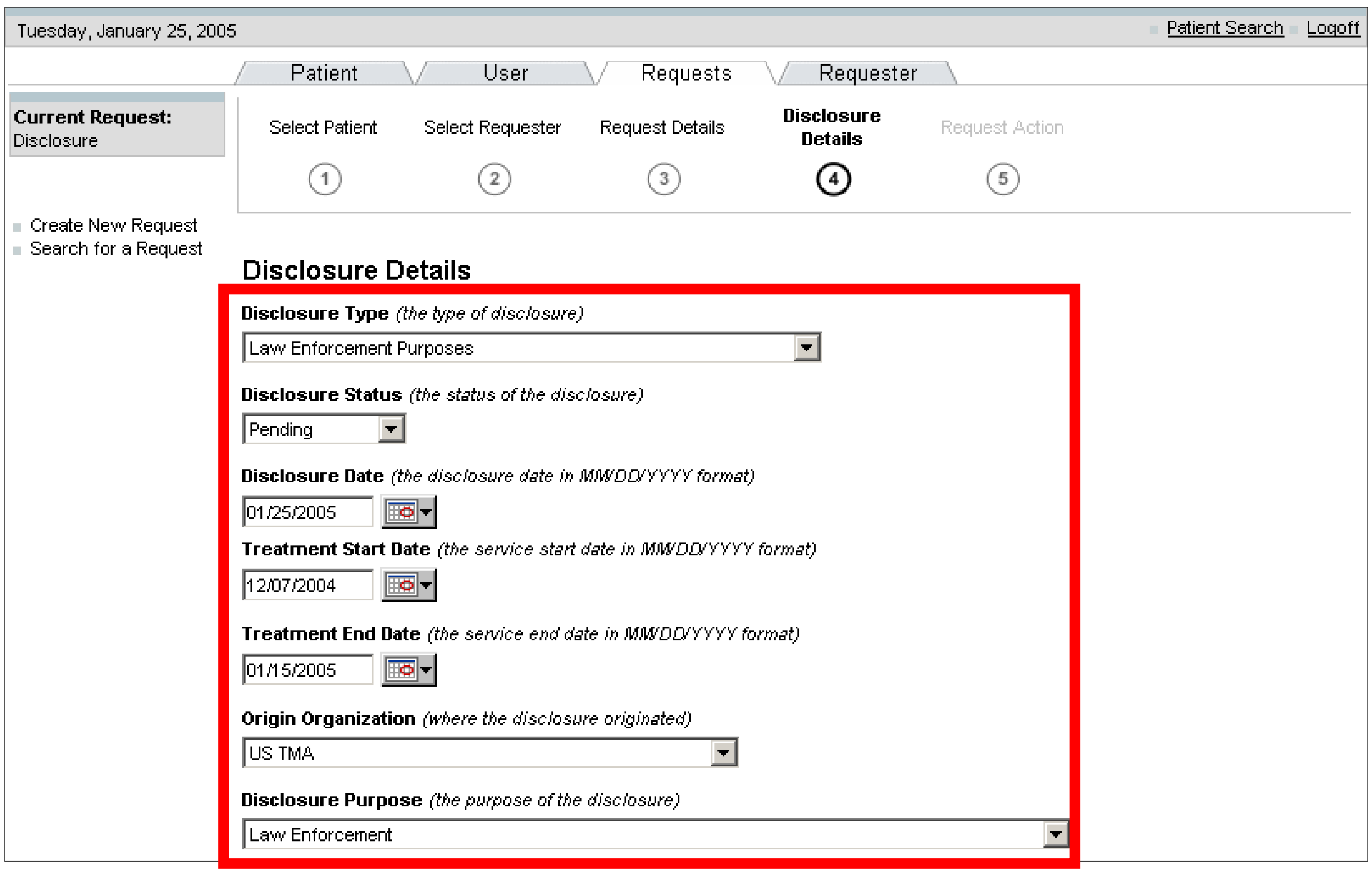
12. Scroll down the screen and enter: (Information start and end date, request format, and request classification)
13. Click on the Next button



Disclosures

Recording a Request for Disclosure (9 of 12)

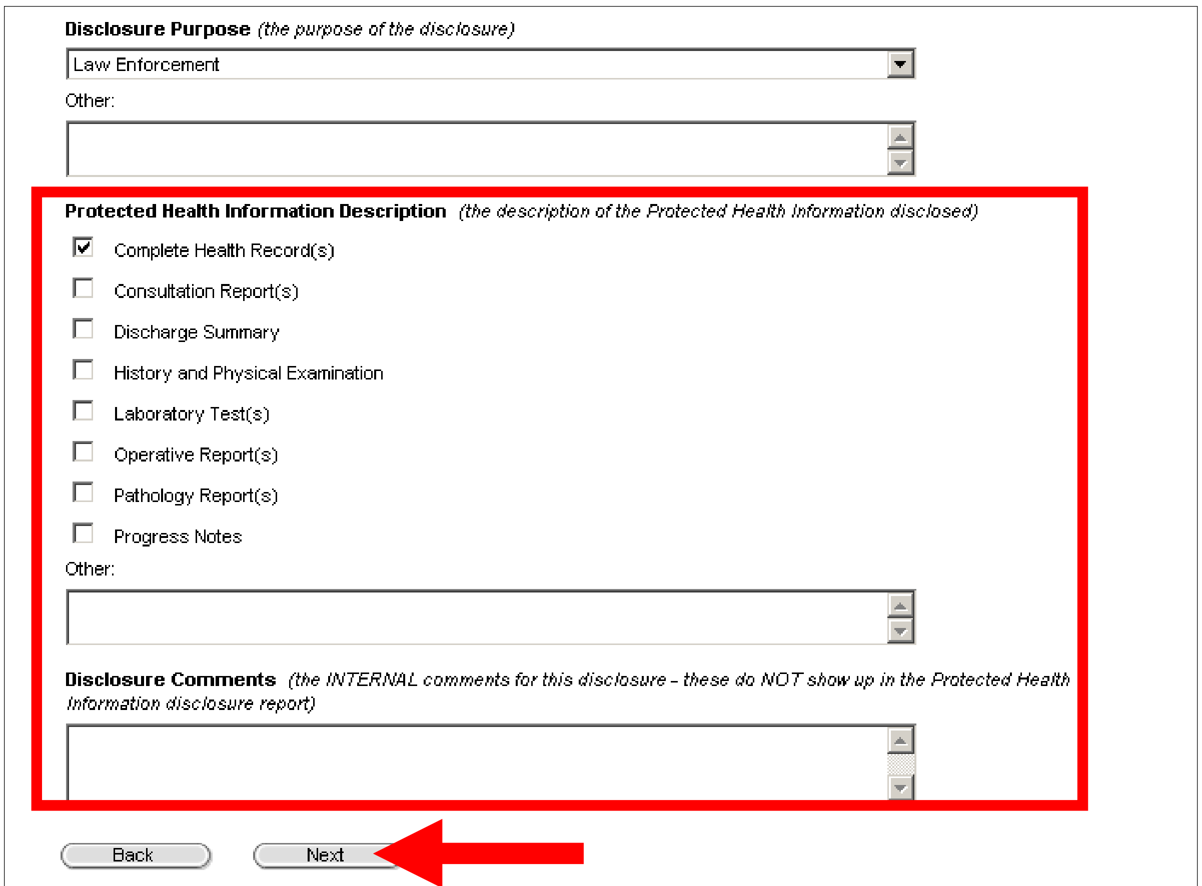
14. Enter in the Disclosure Details: (Disclosure type, status, disclosure date, treatment start and end date, origin organization, disclosure purpose)



Disclosures

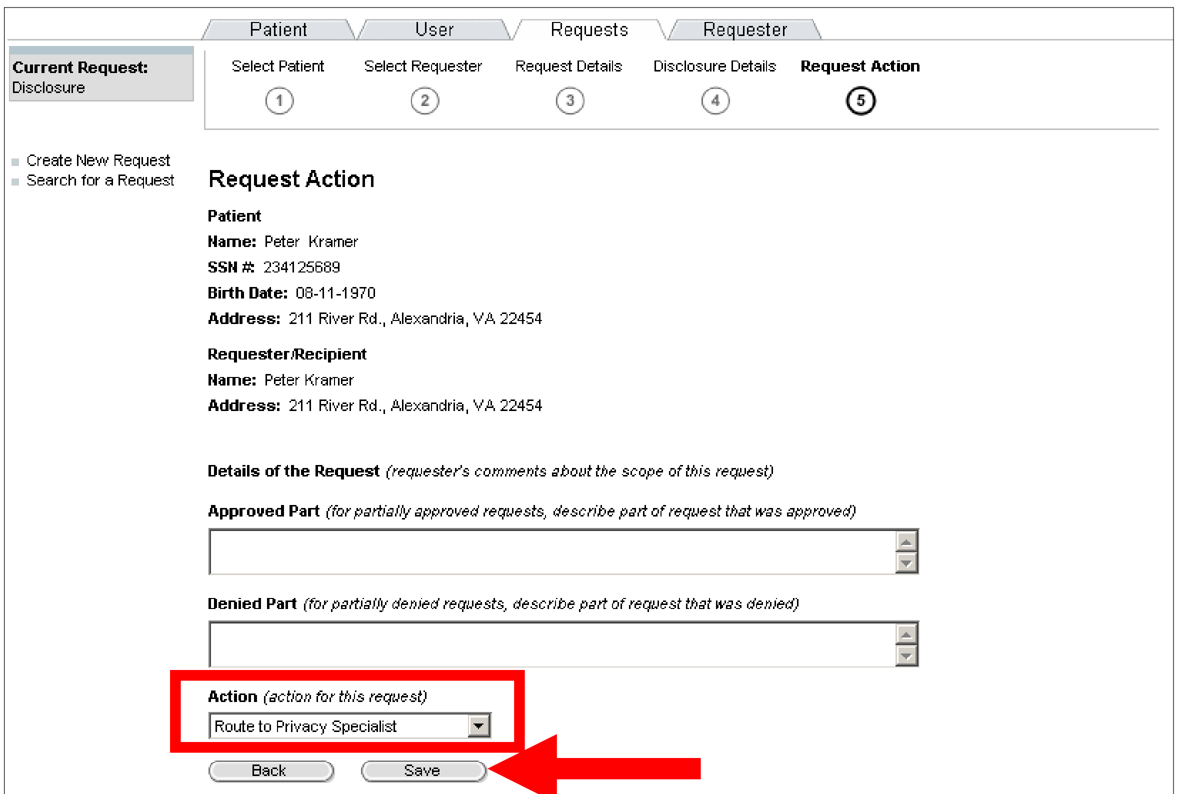
Recording a Request for Disclosure (10 of 12)

15. Scroll down the screen and enter: (PHI description and disclosure comments)
16. Click on the Next button



Recording a Request for Disclosure (11 of 12)

17. Enter in the Request Action Details
18. From the Action drop-down box, select the appropriate routing option (Privacy Specialist)
19. Click on the Save button



Recording a Request for Disclosure (12 of 12)

20. The Disclosure Request Summary will display

Tuesday, January 25, 2005 | Patient Search | Logoff

Patient | User | Requests | Requester

Current Request:
Disclosure

Summary
History
Documents
Request Details
Disclosure Details
Request Action

- Create New Request
- Search for a Request

Request Summary

Patient

Name: Peter Kramer

SSN #: 234125689

Birth Date: 08-11-1970

Address: 211 River Rd., Alexandria, VA 22454

Requester/Recipient

Name: Peter Kramer

Address: 211 River Rd., Alexandria, VA 22454

Request Status: Routed for Approval

Request Creation Date: 01/25/2005 at 04:06:05 PM EST

Request Last Update Date: 01/25/2005 at 04:06:06 PM EST

Other Request Details

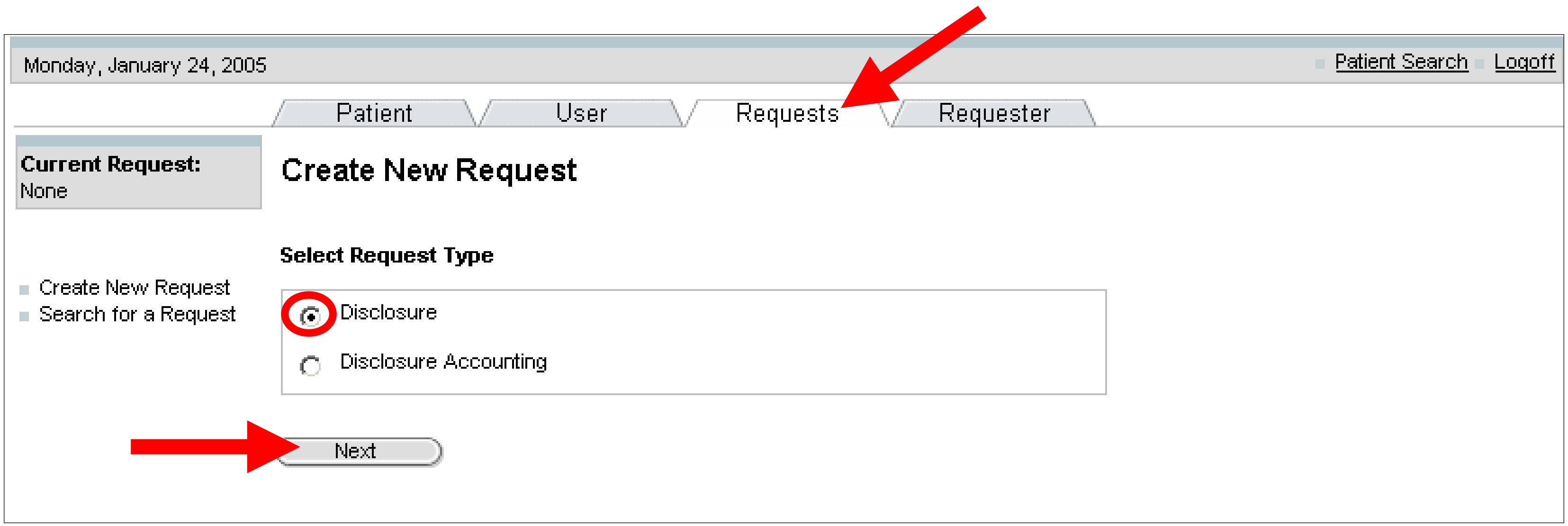
Description	Details
Request Type	Disclosure
Details of the Request	
Disclosure Type	Type: Law Enforcement Purposes, ID: 268, Date: 01/25/2005
Start Date	01/25/2005
End Date	02/25/2005
PHI Items	Complete Health Record(s)
Authority Verified	Patient is Requester

Update Patient Address (1 of 6)

- For a disclosure to be valid, a patient’s address must be entered
- The Regular User can update the patient’s address in the middle of the disclosure request

Update Patient Address (2 of 6)

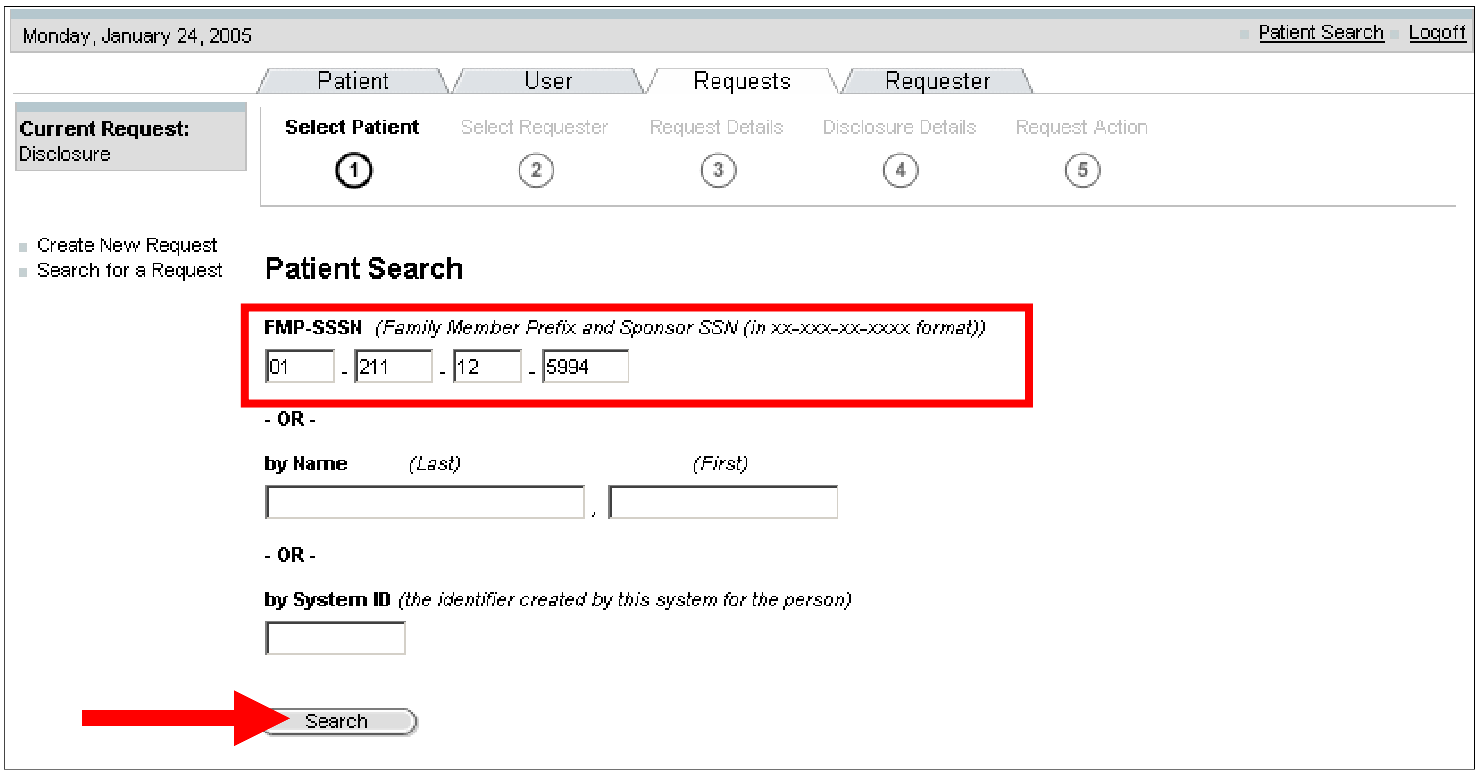
1. Click on the Request Tab
2. Select the Disclosure radio button
3. Click on the Next button



Disclosures

Update Patient Address (3 of 6)

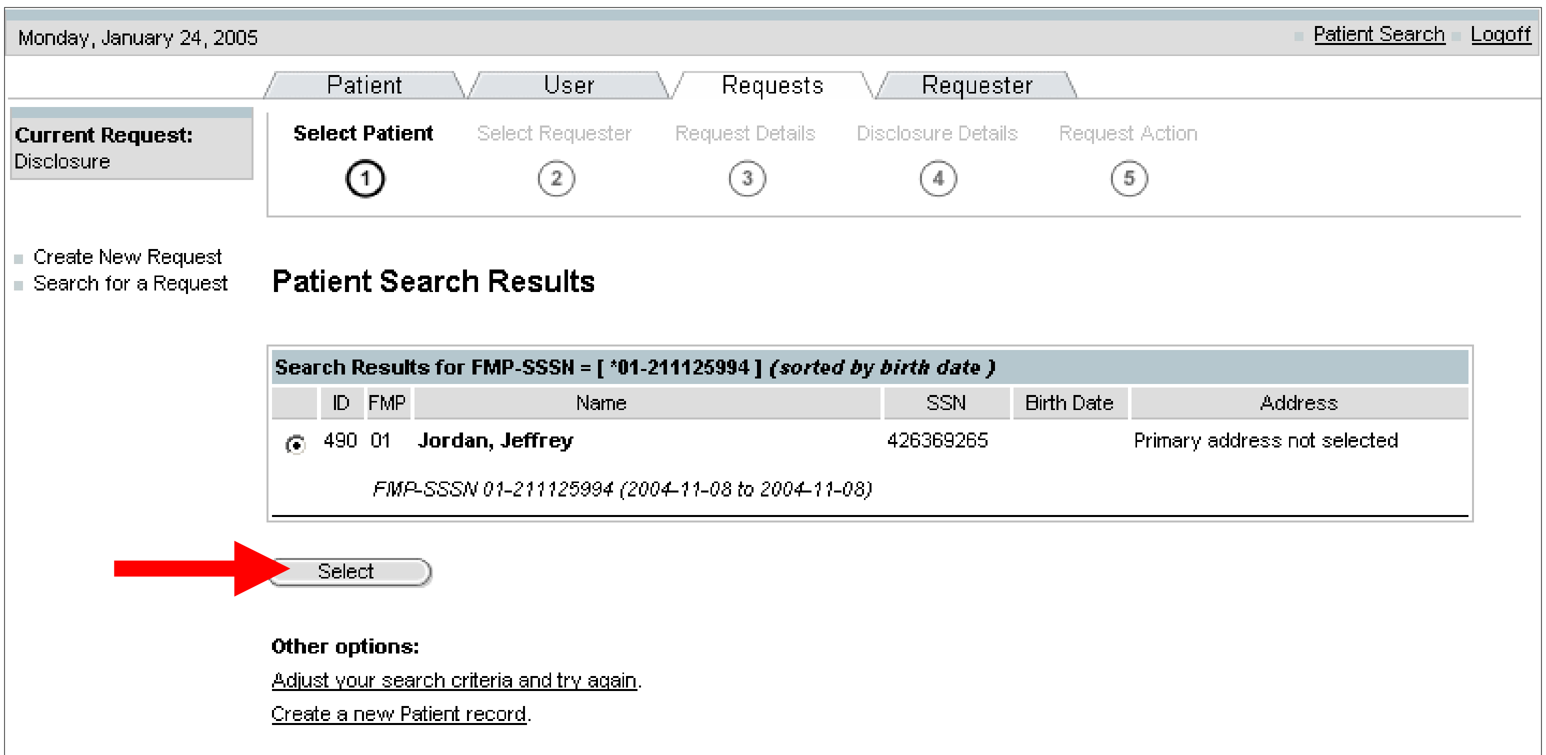
4. Type in the patient's FMP-SSSN
5. Click on the Search button



Update Patient Address (4 of 6)

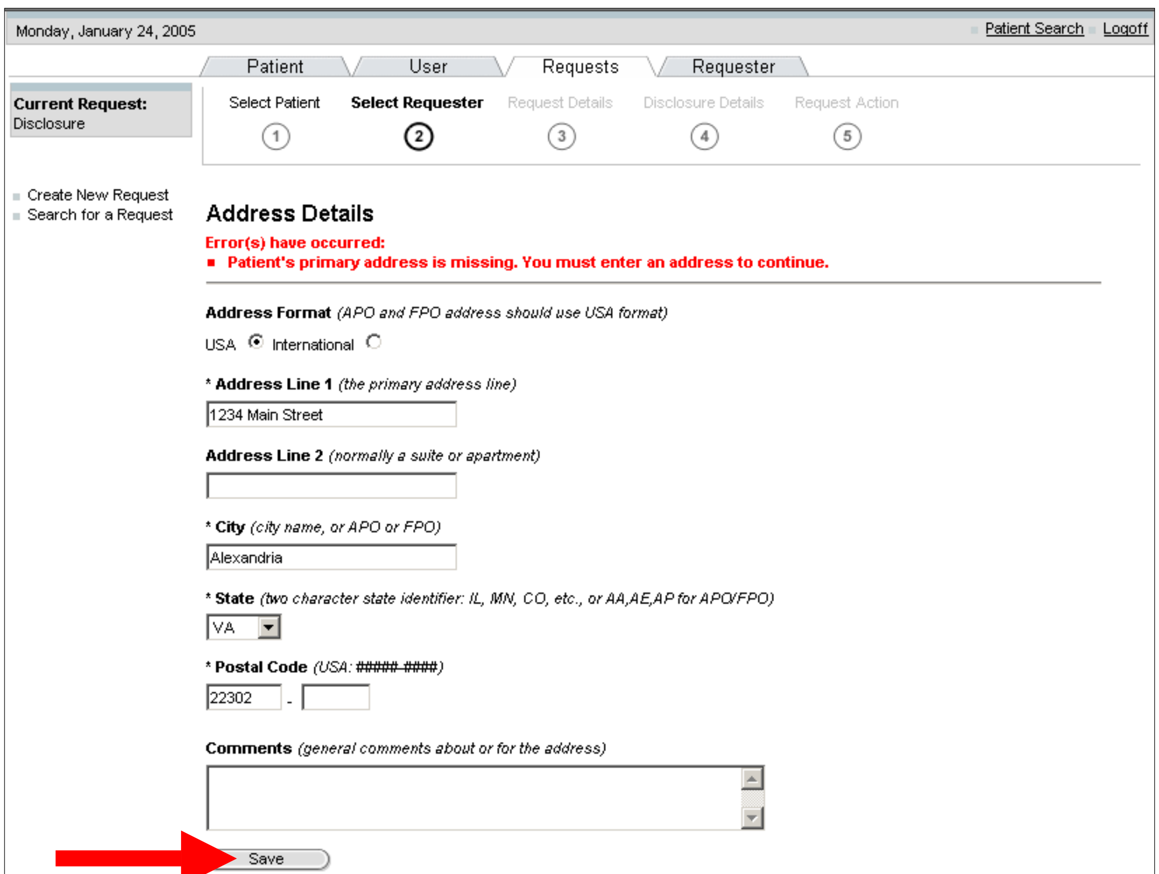
- The primary address is not entered

6. Select the patient



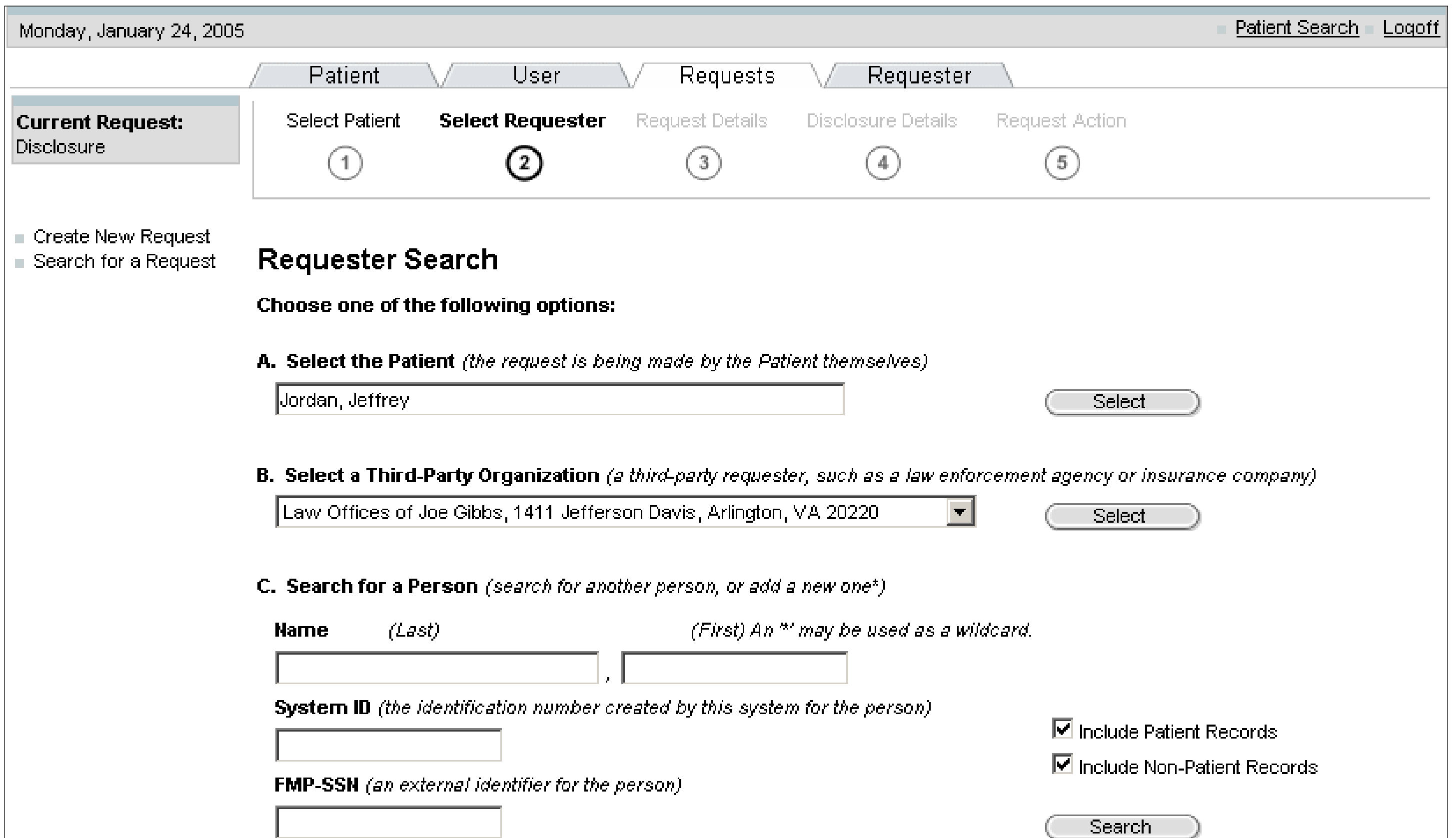
Update Patient Address (5 of 6)

7. Type in the patient’s address
8. Click on the Save button



Update Patient Address (6 of 6)

- After saving the address, you can continue with the Disclosure Request where you left off

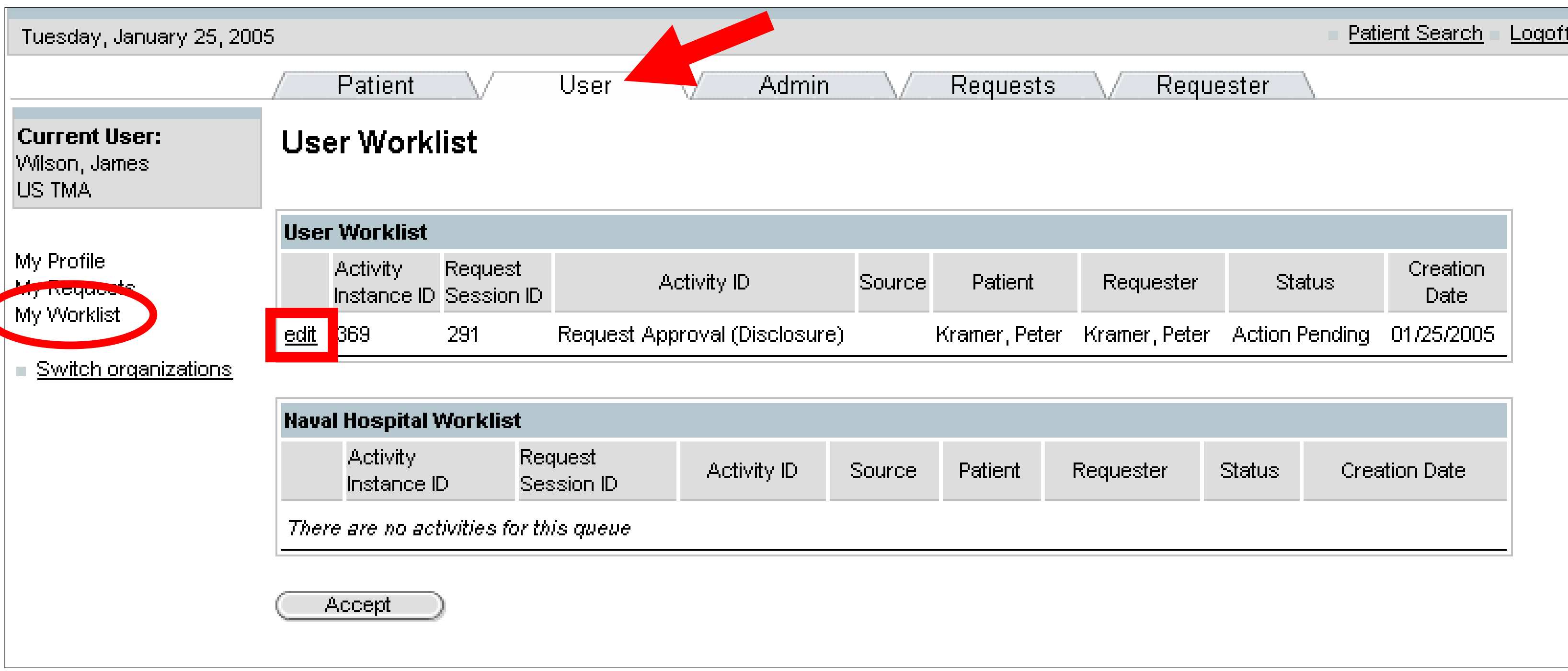


Approving/Denying a Disclosure (1 of 4)

- Once a Regular User routes a request for disclosure to the Privacy Specialist, the request will display in the Privacy Specialist’s work list
- The Privacy Specialist will then approve or deny the request

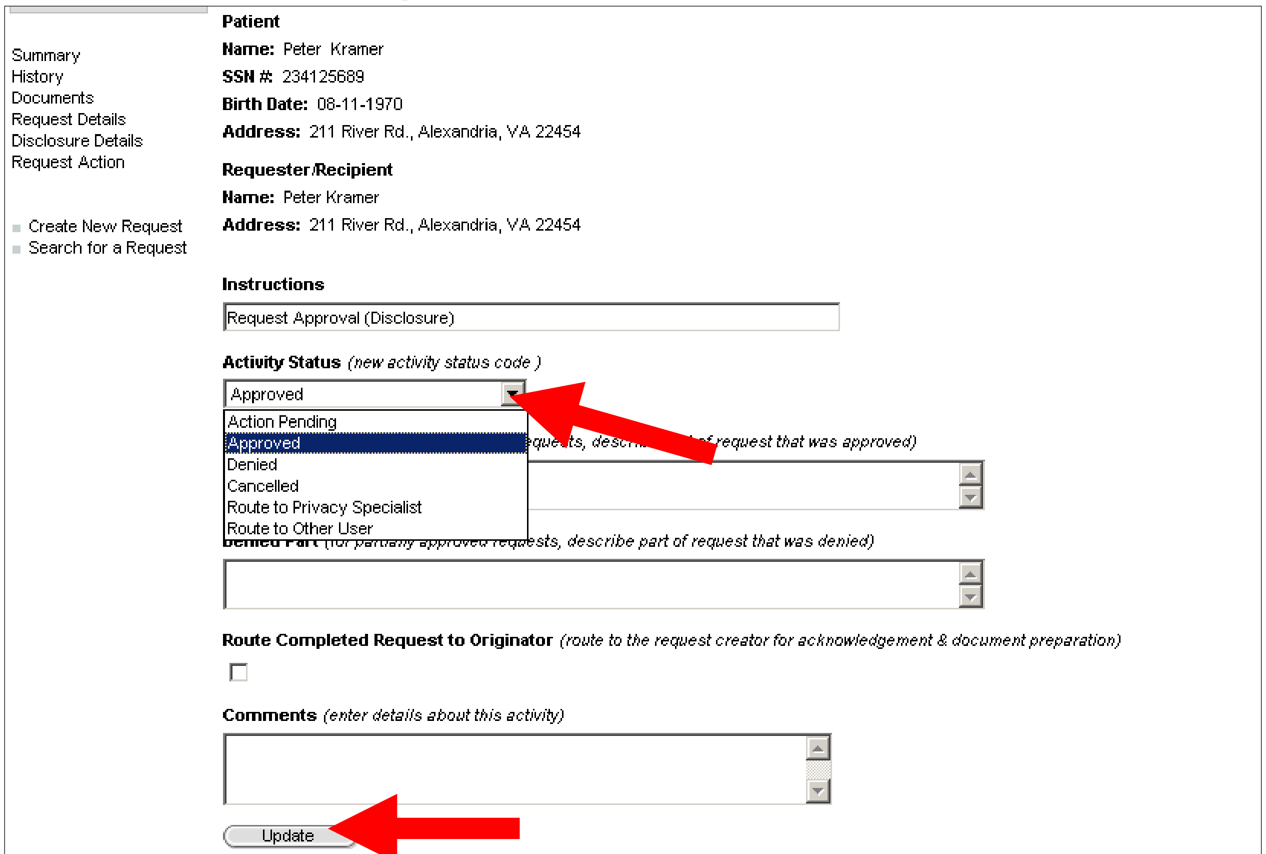
Approving/Denying a Disclosure (2 of 4)

1. Select the User tab
2. Select My Worklist hyperlink
3. Select the Edit hyperlink for the disclosure that the Privacy Specialist will approve or deny



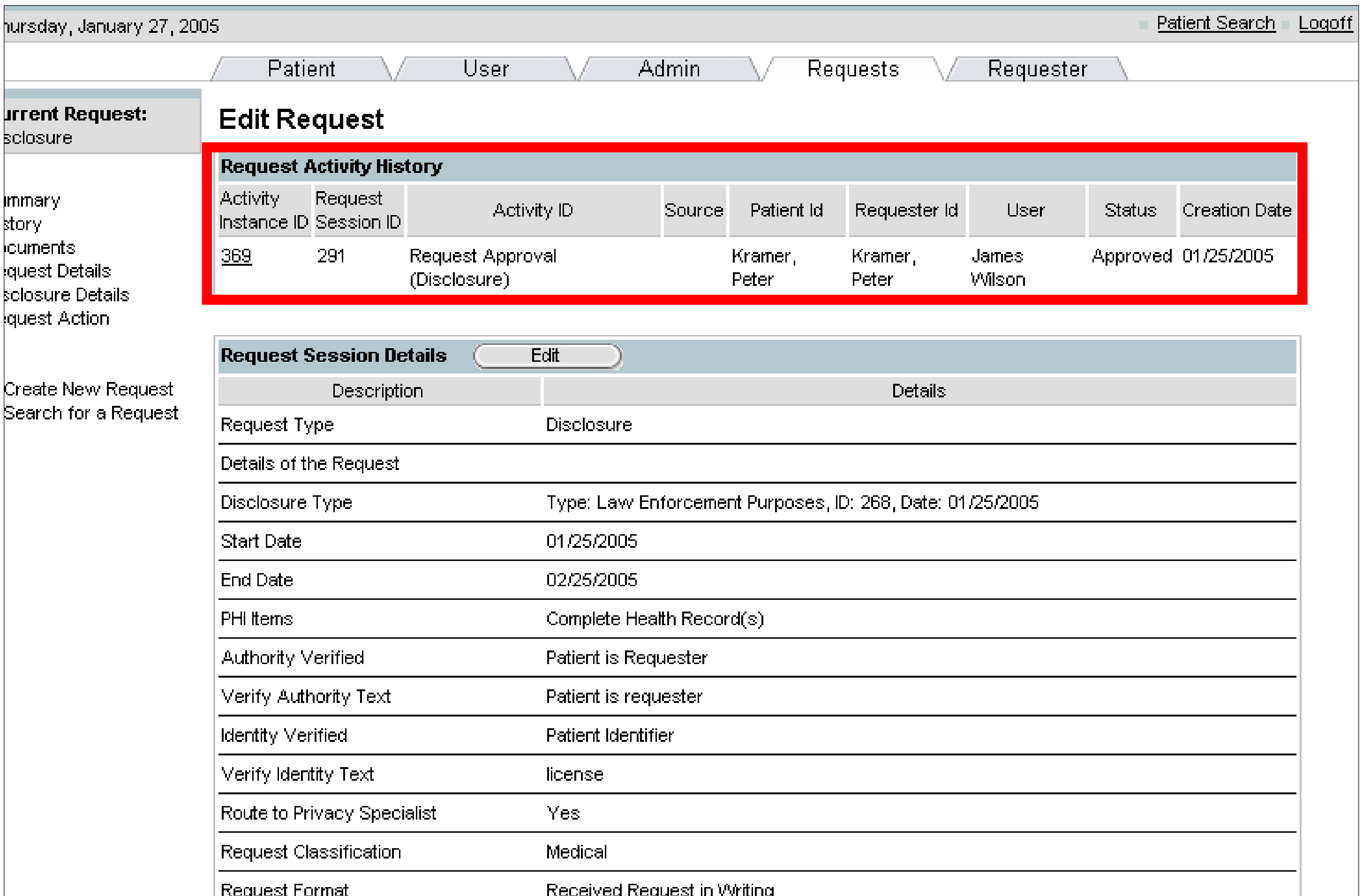
Approving/Denying a Disclosure (3 of 4)

4. Select Approved or Denied from the Activity Status drop-down box
5. Click on the Update button



Approving/Denying a Disclosure (4 of 4)

- The approved/denied request will display in the Request Activity History box



ıursday, January 27, 2005 | Patient Search | Logoff

Patient | User | Admin | Requests | Requester

ırrent Request:
sclosure

ımmary
story
ıcuments
ıquest Details
sclosure Details
ıquest Action

Create New Request
Search for a Request

Edit Request

Request Activity History

Activity Instance ID	Request Session ID	Activity ID	Source	Patient Id	Requester Id	User	Status	Creation Date
369	291	Request Approval (Disclosure)		Kramer, Peter	Kramer, Peter	James Wilson	Approved	01/25/2005

Request Session Details Edit

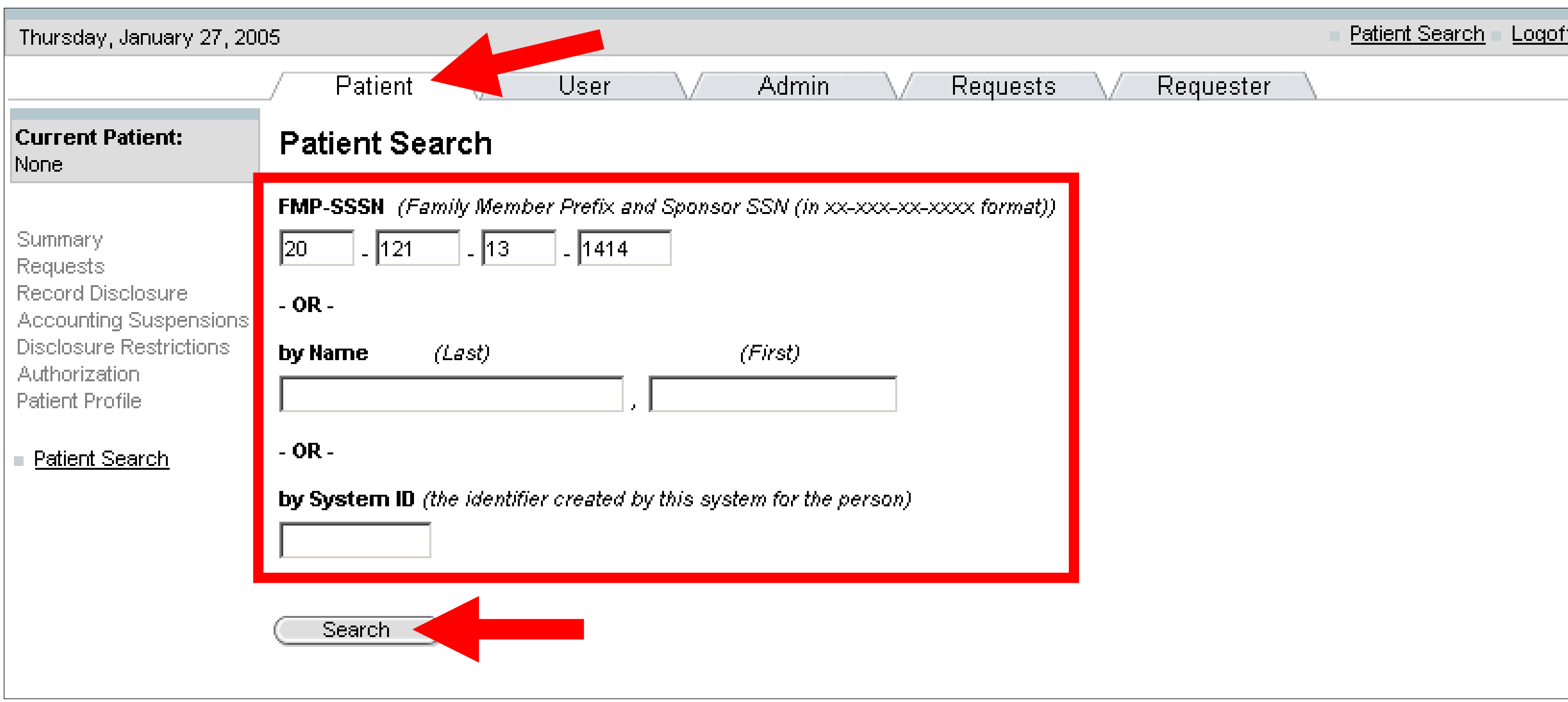
Description	Details
Request Type	Disclosure
Details of the Request	
Disclosure Type	Type: Law Enforcement Purposes, ID: 268, Date: 01/25/2005
Start Date	01/25/2005
End Date	02/25/2005
PHI Items	Complete Health Record(s)
Authority Verified	Patient is Requester
Verify Authority Text	Patient is requester
Identity Verified	Patient Identifier
Verify Identity Text	license
Route to Privacy Specialist	Yes
Request Classification	Medical
Request Format	Received Request in Writing

Recording a Disclosure (1 of 10)

- Privacy Specialists have the ability to record and approve disclosures in one step
- This eliminates the two step process of recording the request, routing it to their work list, and then approving it

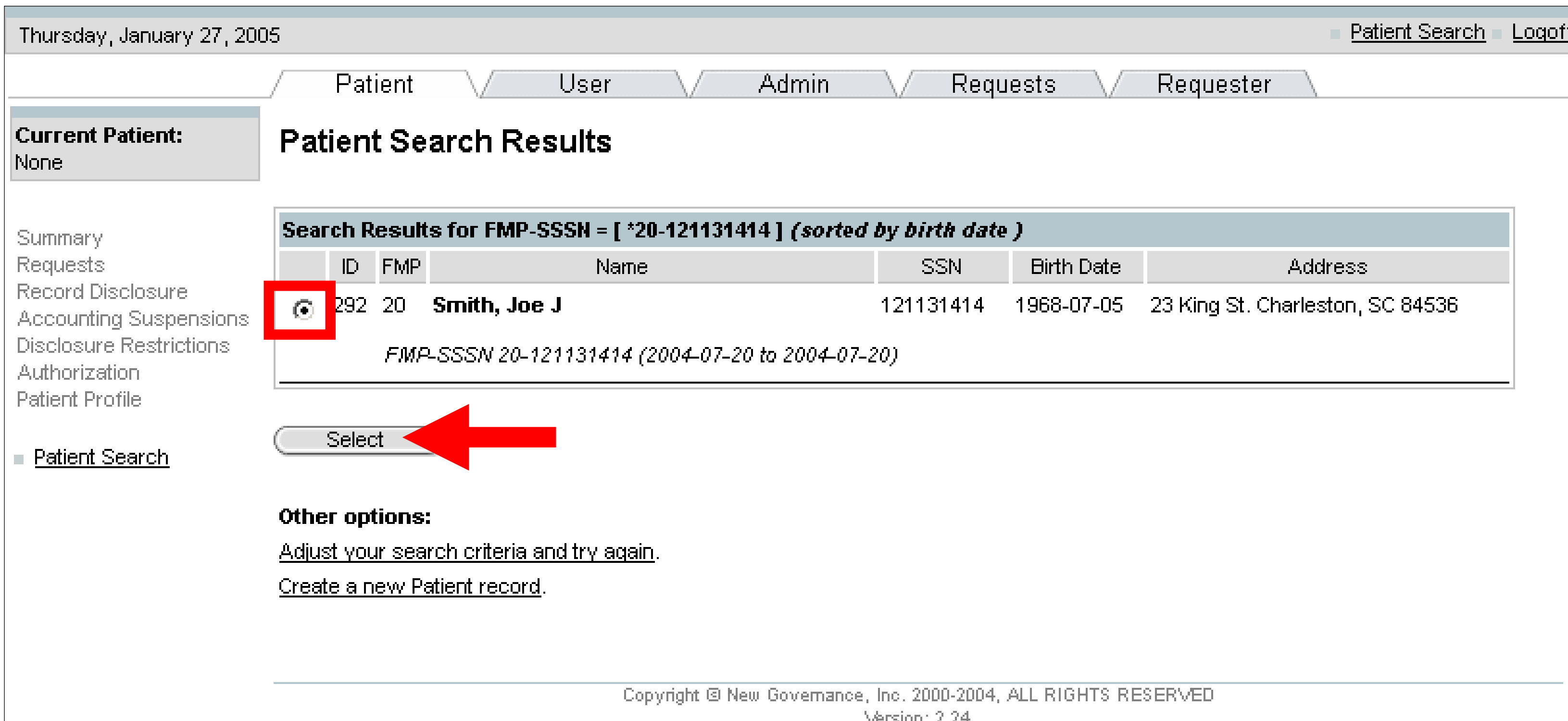
Recording a Disclosure (2 of 10)

1. Select the Patient tab
2. Enter patient search criteria
3. Click on the Search button



Recording a Disclosure (3 of 10)

4. Click on the radio button for the appropriate patient
5. Click on the Select button

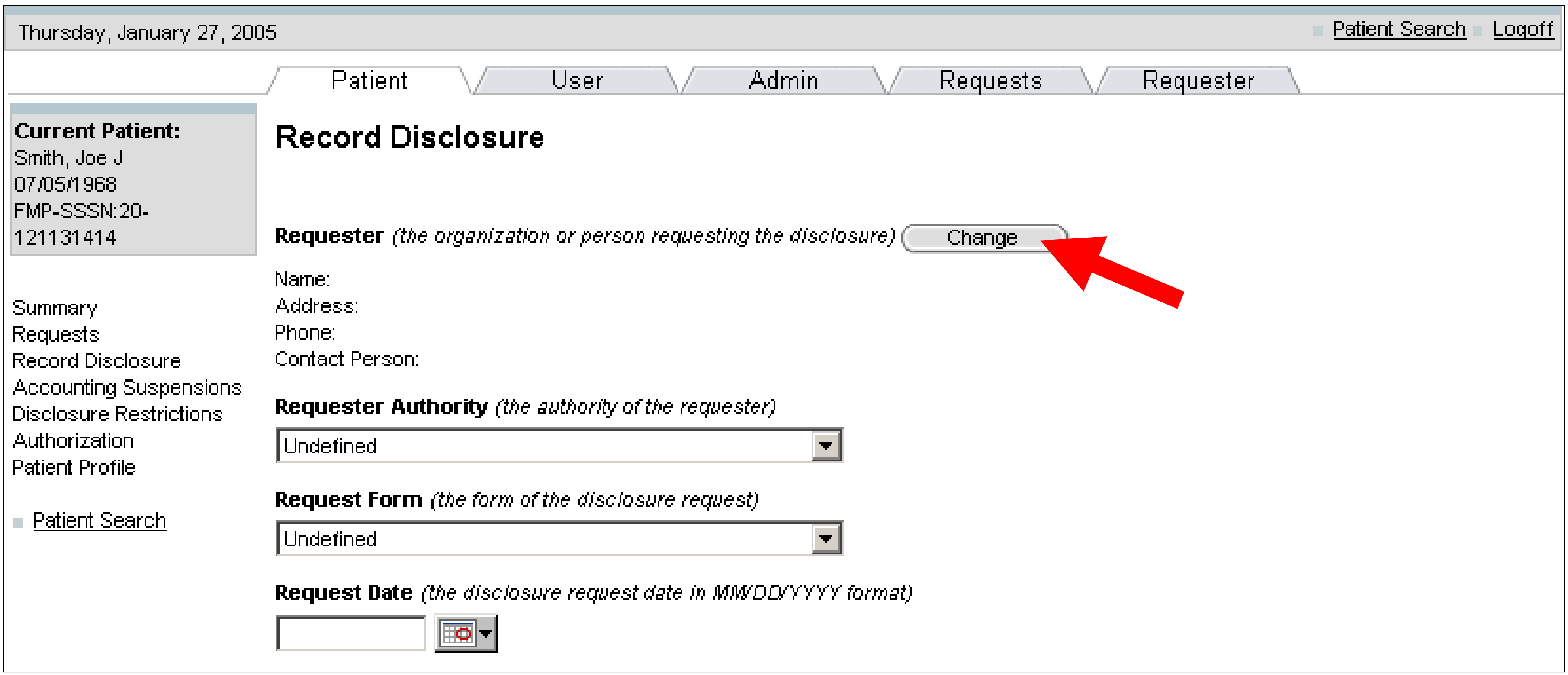


Recording a Disclosure (4 of 10)

6. Select the Record Disclosure hyperlink

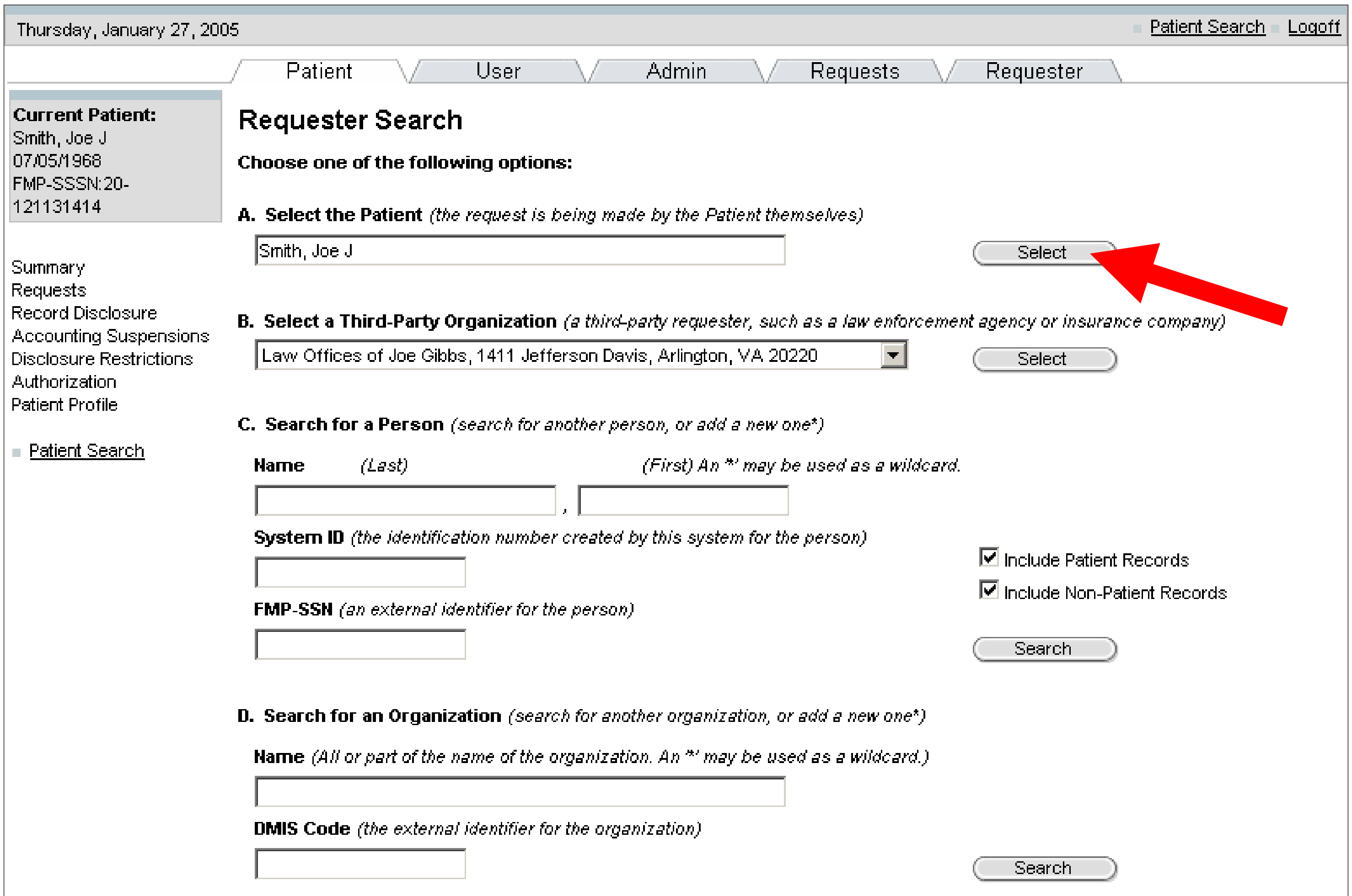
Recording a Disclosure (5 of 10)

7. Click on the Change button to change or update the requester



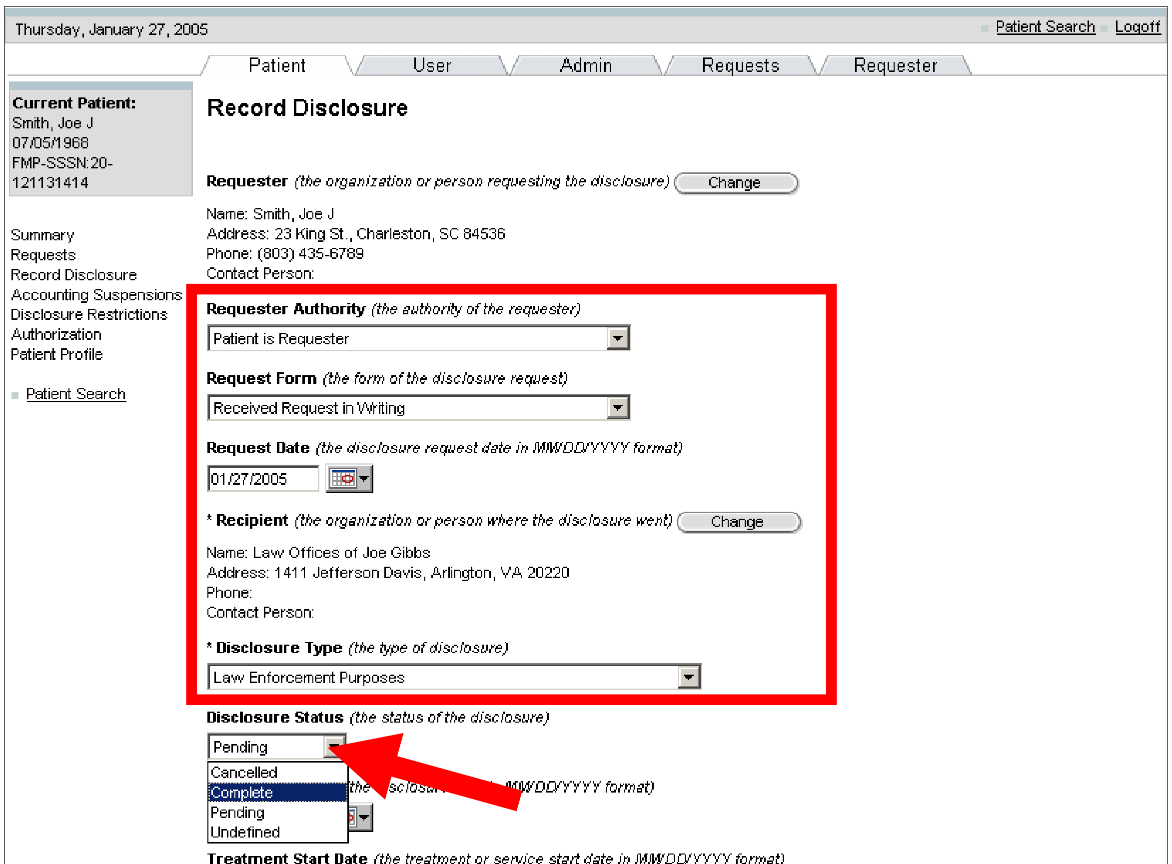
Recording a Disclosure (6 of 10)

8. Select the requester



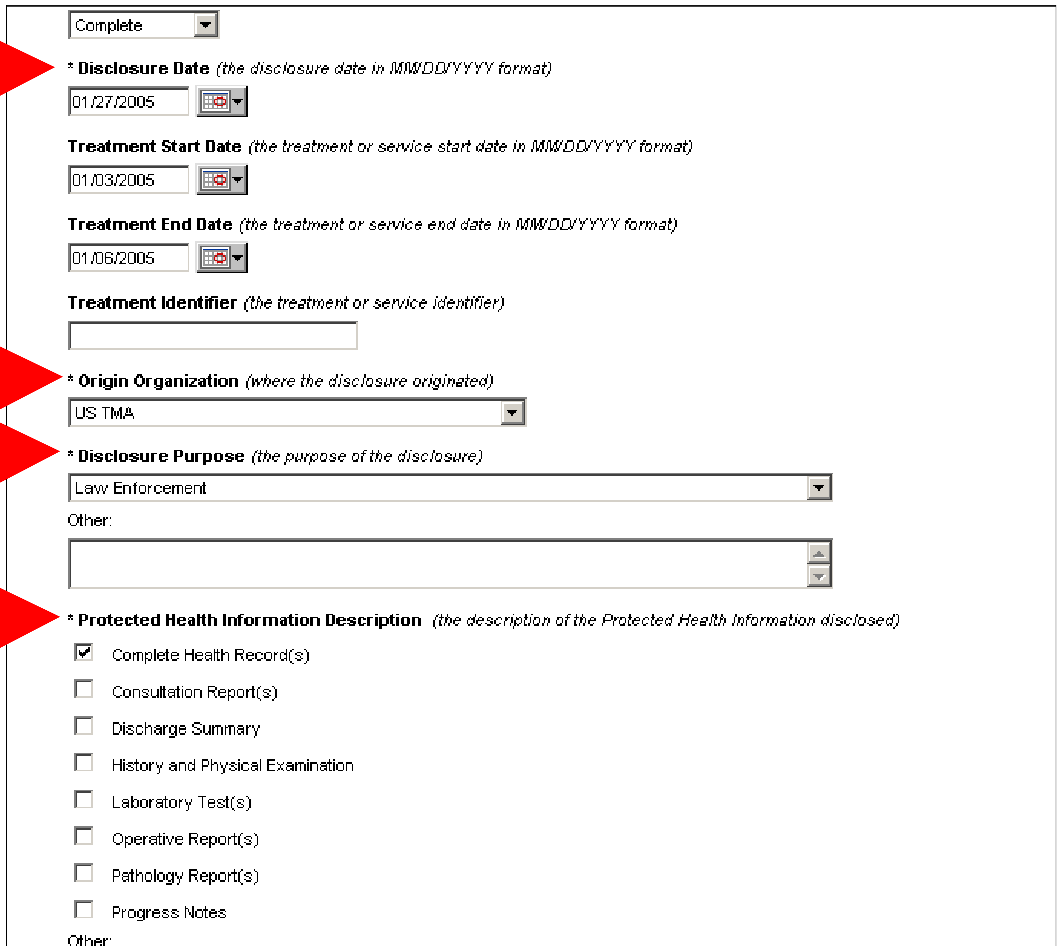
Recording a Disclosure (7 of 10)

9. Record the disclosure details: (requester authority, form, date, recipient, disclosure type)
10. Select the Disclosure Status from the drop-down box



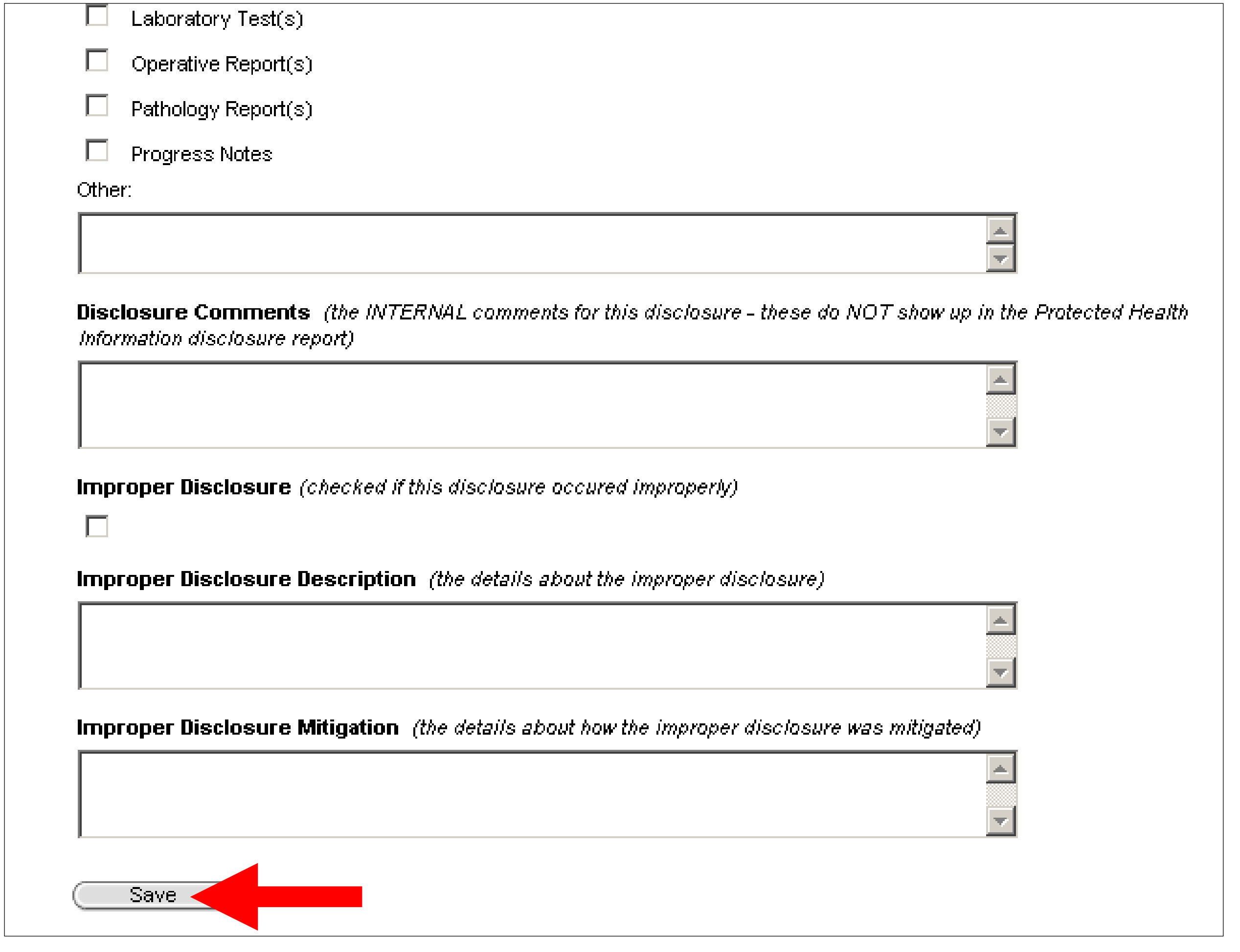
Recording a Disclosure (8 of 10)

11. Scroll down the screen and enter: (disclosure date, origin organization, disclosure purpose, and PHI description)



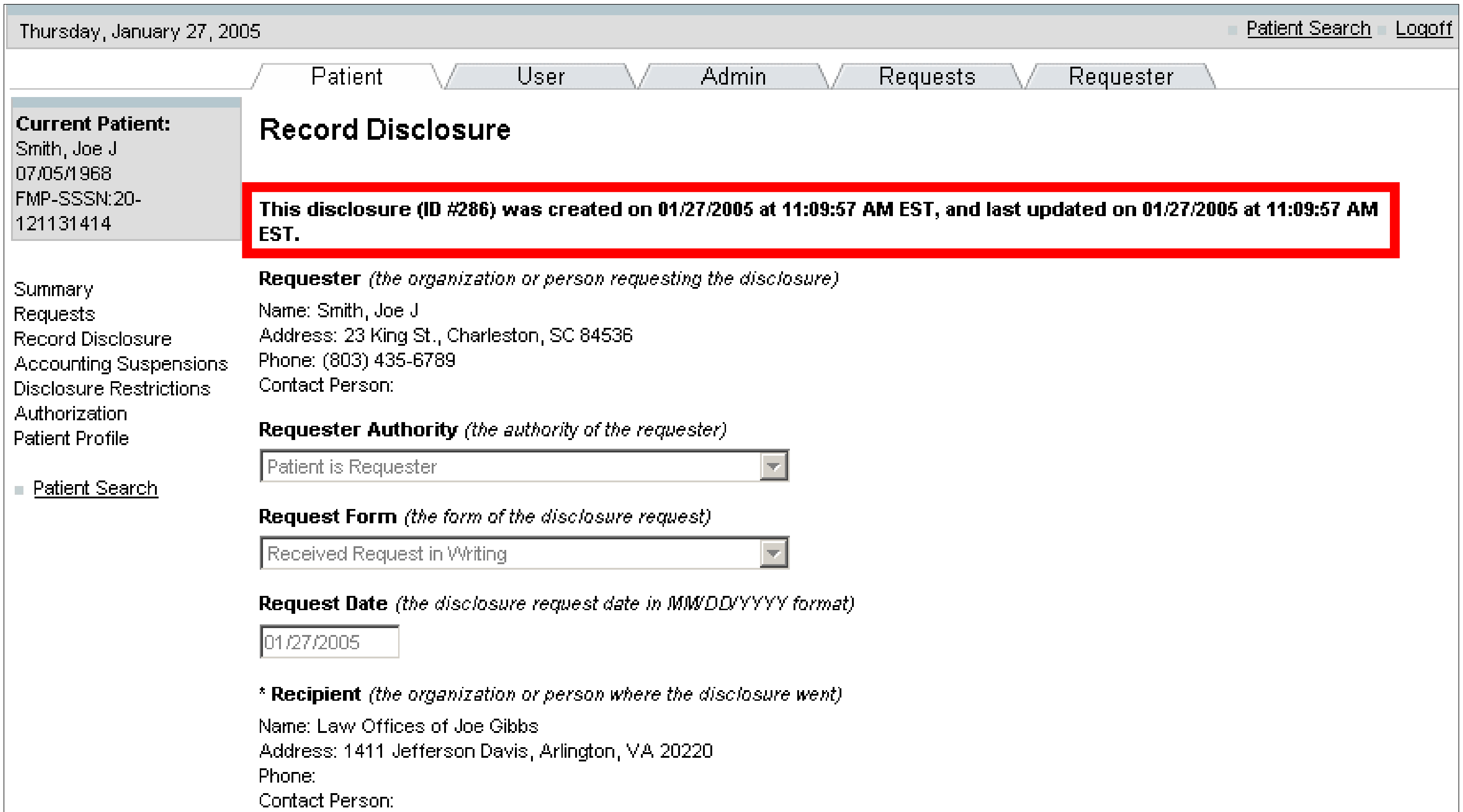
Recording a Disclosure (9 of 10)

12. Scroll down to the bottom of the screen and click on the Save button



Recording a Disclosure (10 of 10)

- The disclosure is now complete and only the disclosure comments and improper fields can be updated



Thursday, January 27, 2005

Patient Search Logoff

Patient | User | Admin | Requests | Requester

Current Patient:
Smith, Joe J
07/05/1968
FMP-SSSN:20-121131414

Summary
Requests
Record Disclosure
Accounting Suspensions
Disclosure Restrictions
Authorization
Patient Profile

Patient Search

Record Disclosure

This disclosure (ID #286) was created on 01/27/2005 at 11:09:57 AM EST, and last updated on 01/27/2005 at 11:09:57 AM EST.

Requester *(the organization or person requesting the disclosure)*

Name: Smith, Joe J
Address: 23 King St., Charleston, SC 84536
Phone: (803) 435-6789
Contact Person:

Requester Authority *(the authority of the requester)*

Patient is Requester

Request Form *(the form of the disclosure request)*

Received Request in Writing

Request Date *(the disclosure request date in MM/DD/YYYY format)*

01/27/2005

* **Recipient** *(the organization or person where the disclosure went)*

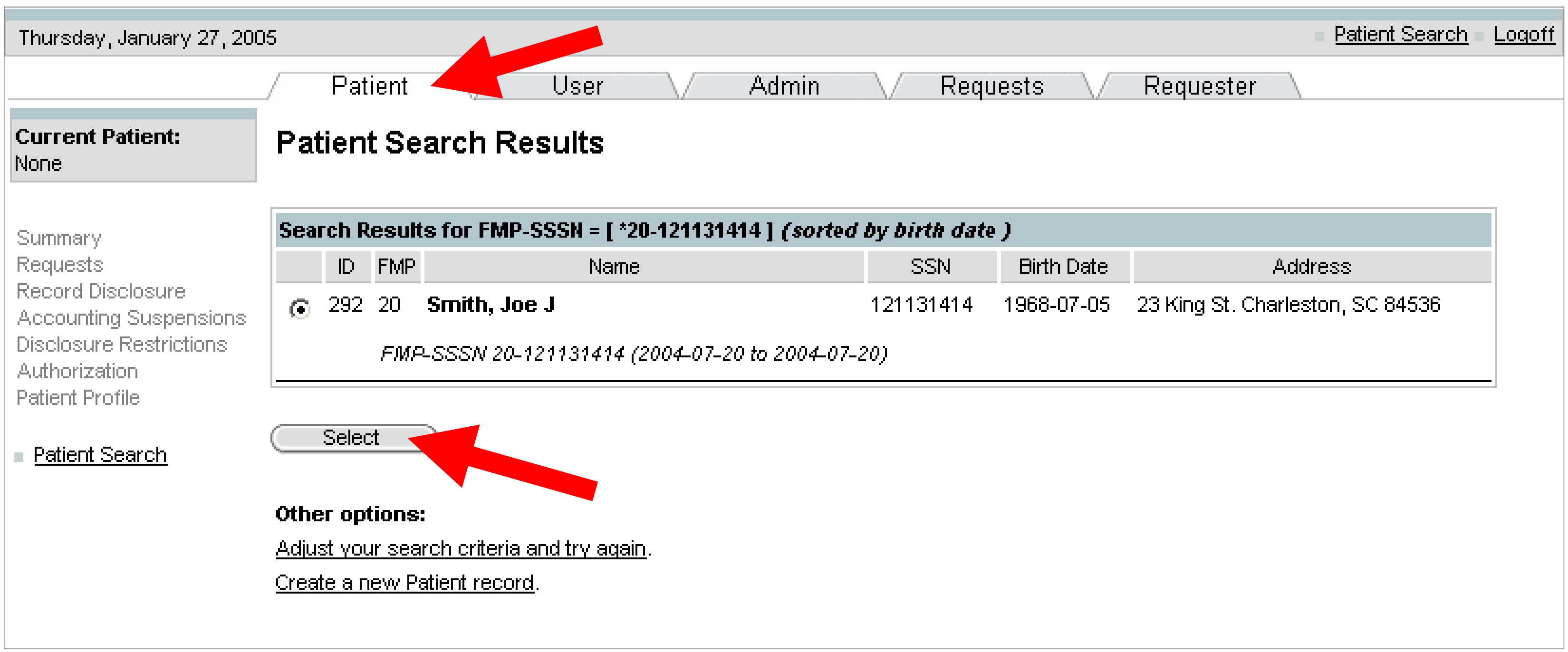
Name: Law Offices of Joe Gibbs
Address: 1411 Jefferson Davis, Arlington, VA 20220
Phone:
Contact Person:

Amending Disclosures (1 of 6)

- As a Privacy Specialist you are authorized to label a disclosure as Improper
- Once a Disclosure status is marked as completed, it can only be amended by marking it as an Improper Disclosure
  - The disclosure was made incorrectly

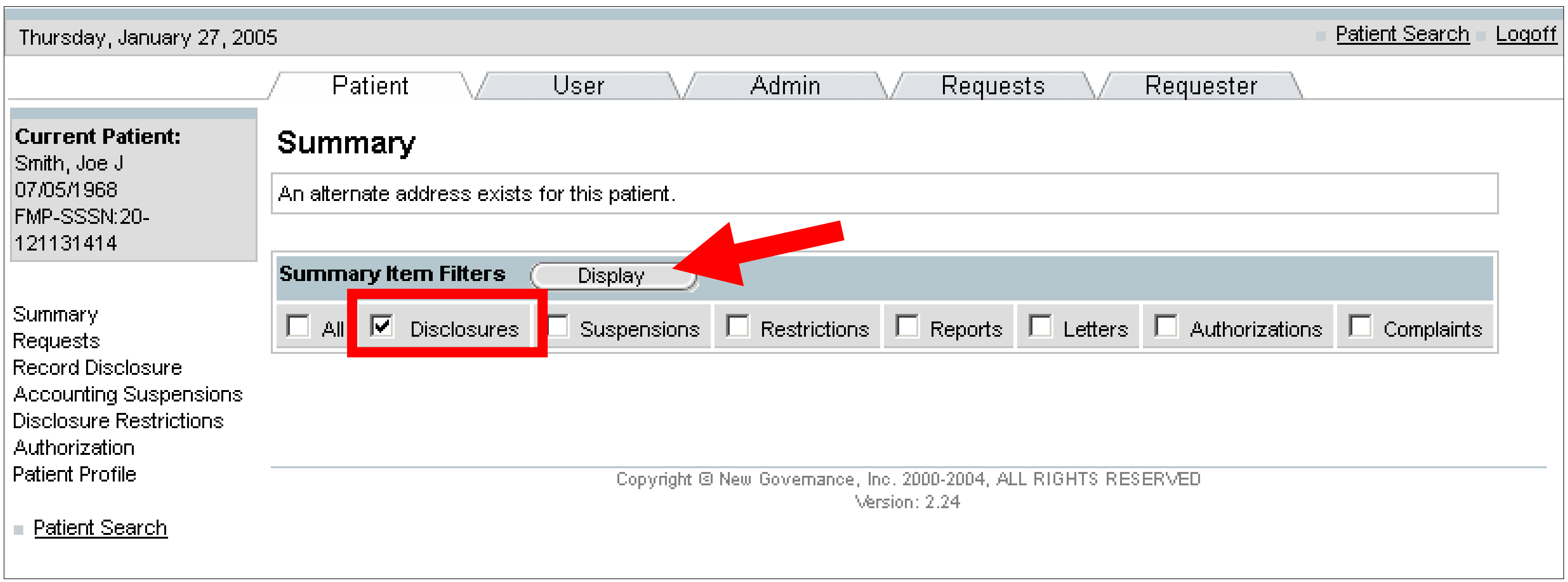
Amending Disclosures (2 of 6)

1. Select the Patient tab
2. Search for and select the patient



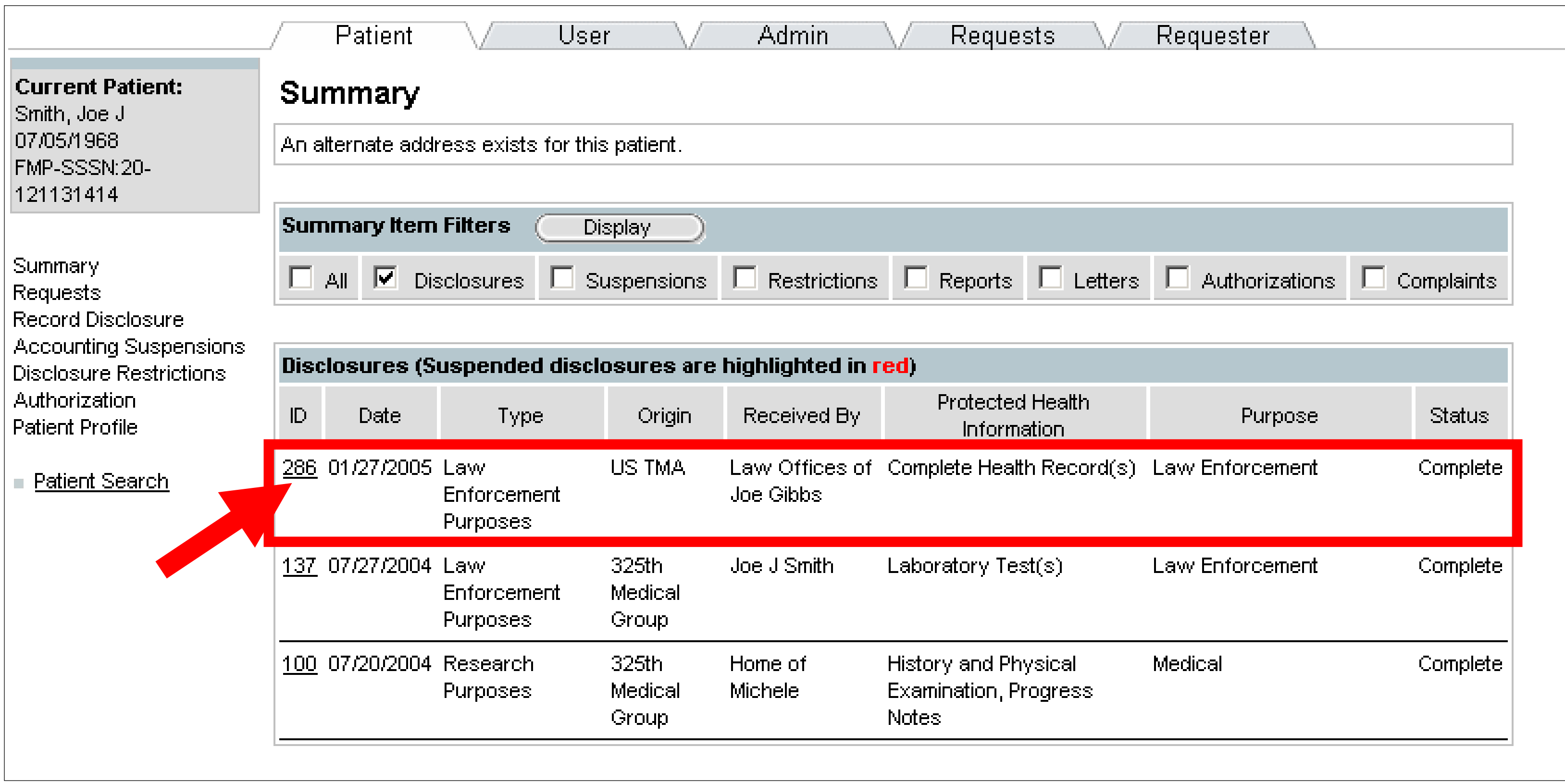
Amending Disclosures (3 of 6)

3. Place a check in the Disclosures box and click on the Display button



Amending Disclosures (4 of 6)

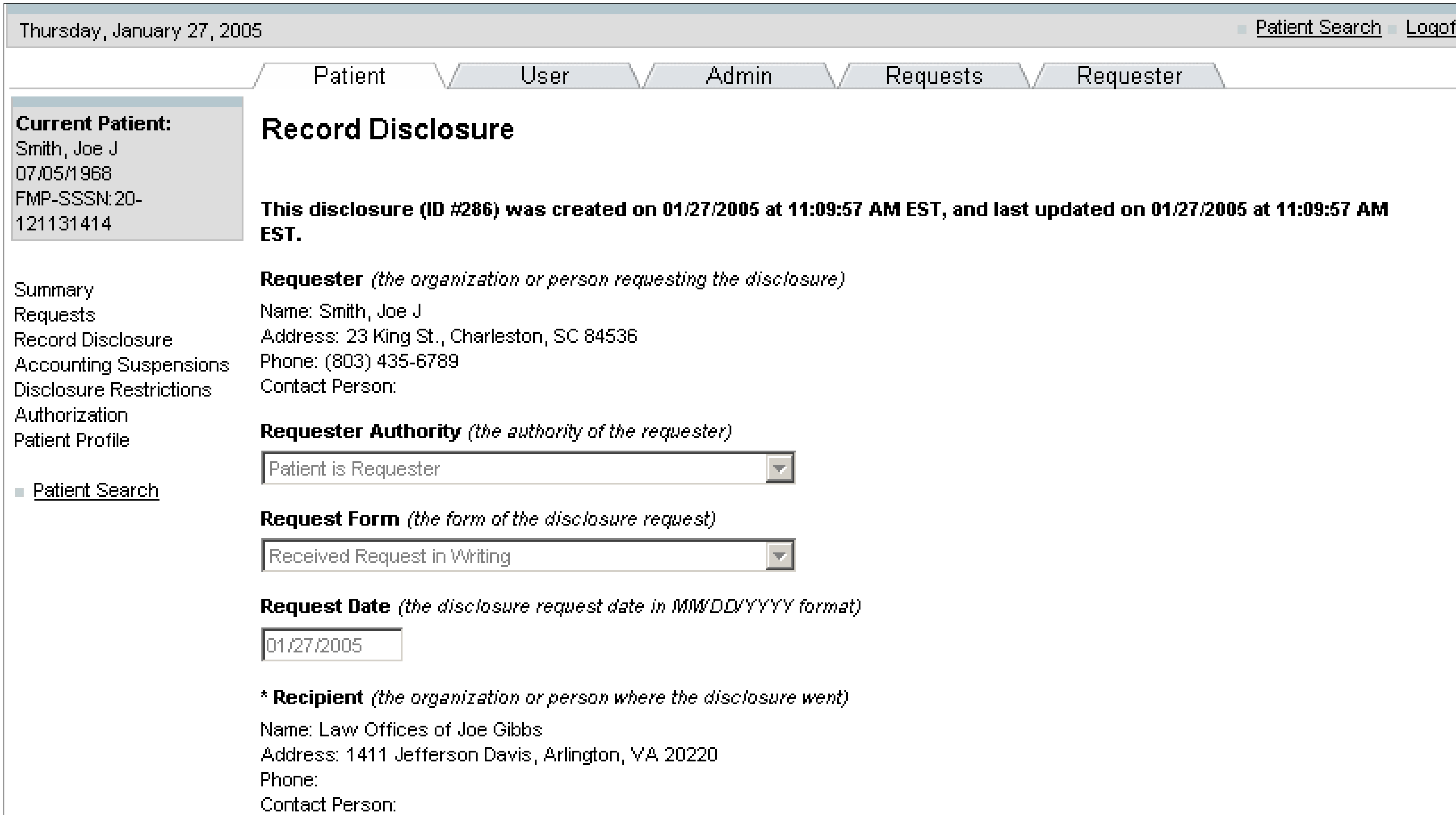
4. Select the ID hyperlink for the disclosure that you want to amend



ID	Date	Type	Origin	Received By	Protected Health Information	Purpose	Status
286	01/27/2005	Law Enforcement Purposes	US TMA	Law Offices of Joe Gibbs	Complete Health Record(s)	Law Enforcement	Complete
137	07/27/2004	Law Enforcement Purposes	325th Medical Group	Joe J Smith	Laboratory Test(s)	Law Enforcement	Complete
100	07/20/2004	Research Purposes	325th Medical Group	Home of Michele	History and Physical Examination, Progress Notes	Medical	Complete

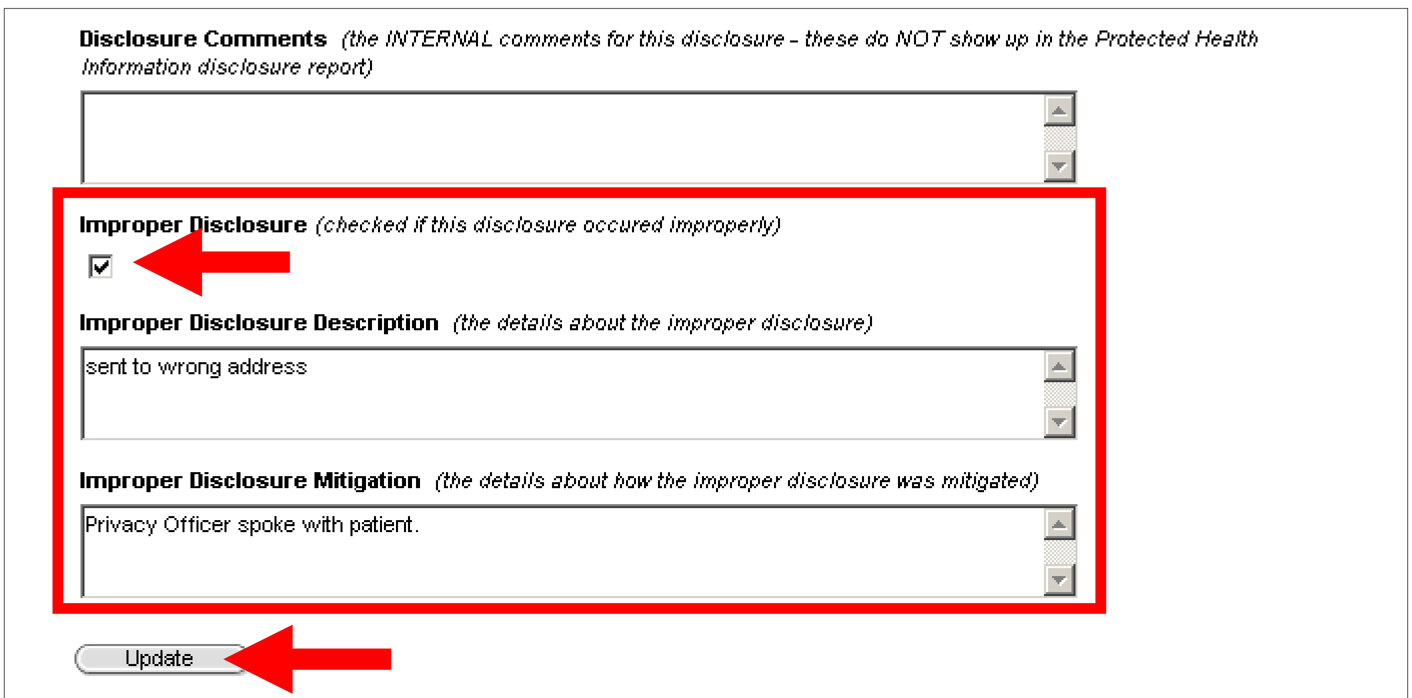
Amending Disclosures (5 of 6)

5. The Record Disclosure screen will display



Amending Disclosures (6 of 6)

6. Scroll to the bottom of the screen and place a check in the Improper Disclosure checkbox
7. Enter a description of the Improper Disclosure and mitigation
8. Click on the Update button



Summary

- You should now be able to:
  - Record a request for disclosure as a Regular User
  - Record a disclosure as a Privacy Specialist
  - Approve/deny the disclosure
  - Amend a disclosure

Accounting of Disclosures

Objectives

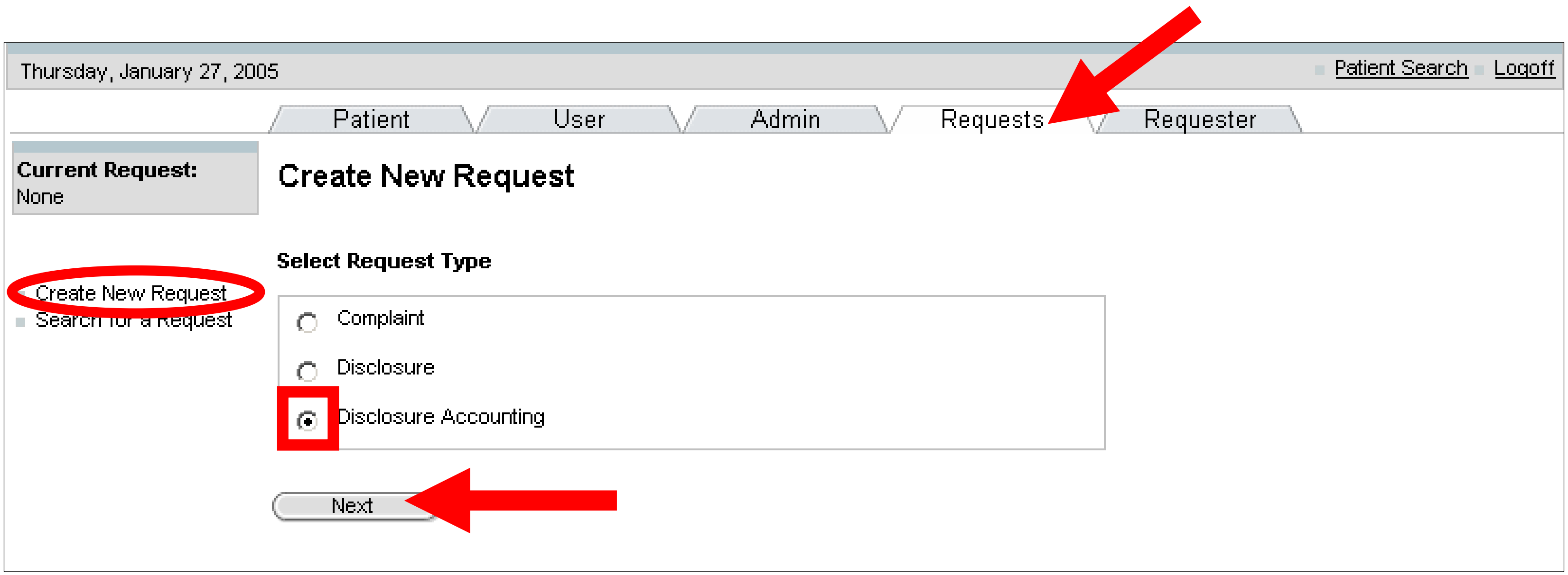
- Once you have completed this lesson, you will be able to:
  - Record a request for an accounting of disclosures
  - Approve/deny a request for an accounting of disclosures
  - Generate an accounting of disclosures report

Recording a Request (1 of 9)

- An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity in the 6 years prior to the date that the accounting is requested
  - DoD 6025.18-R Chapter 13
- Regular Users and Privacy Specialists can record a request for an accounting of disclosures
- Only Privacy Specialists can approve or deny the request

Recording a Request (2 of 9)

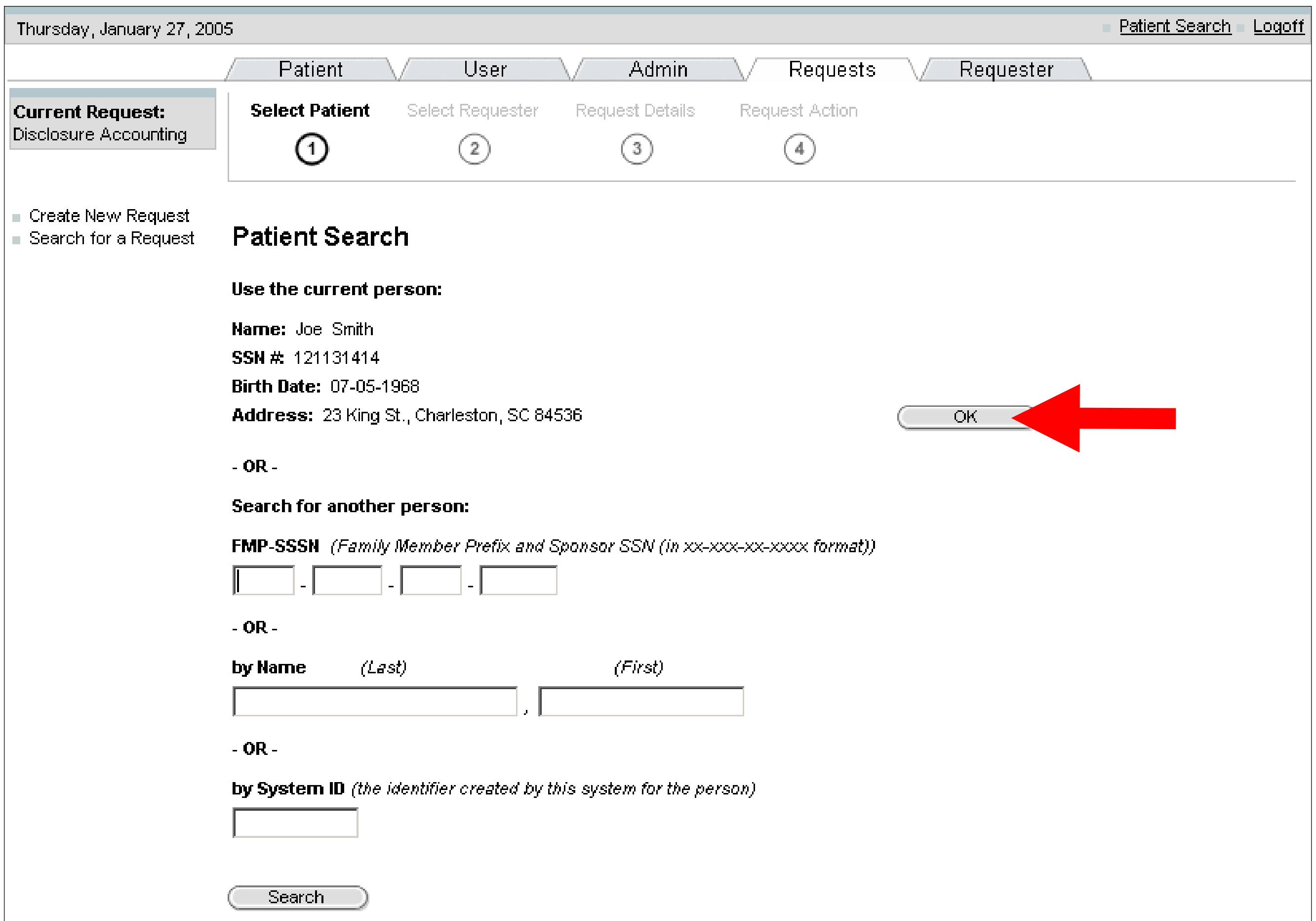
1. Select the Requests Tab
2. Select Create New Request hyperlink and/or click on the radio button for Disclosure Accounting
3. Click on the Next button



Accounting of Disclosures

Recording a Request (3 of 9)

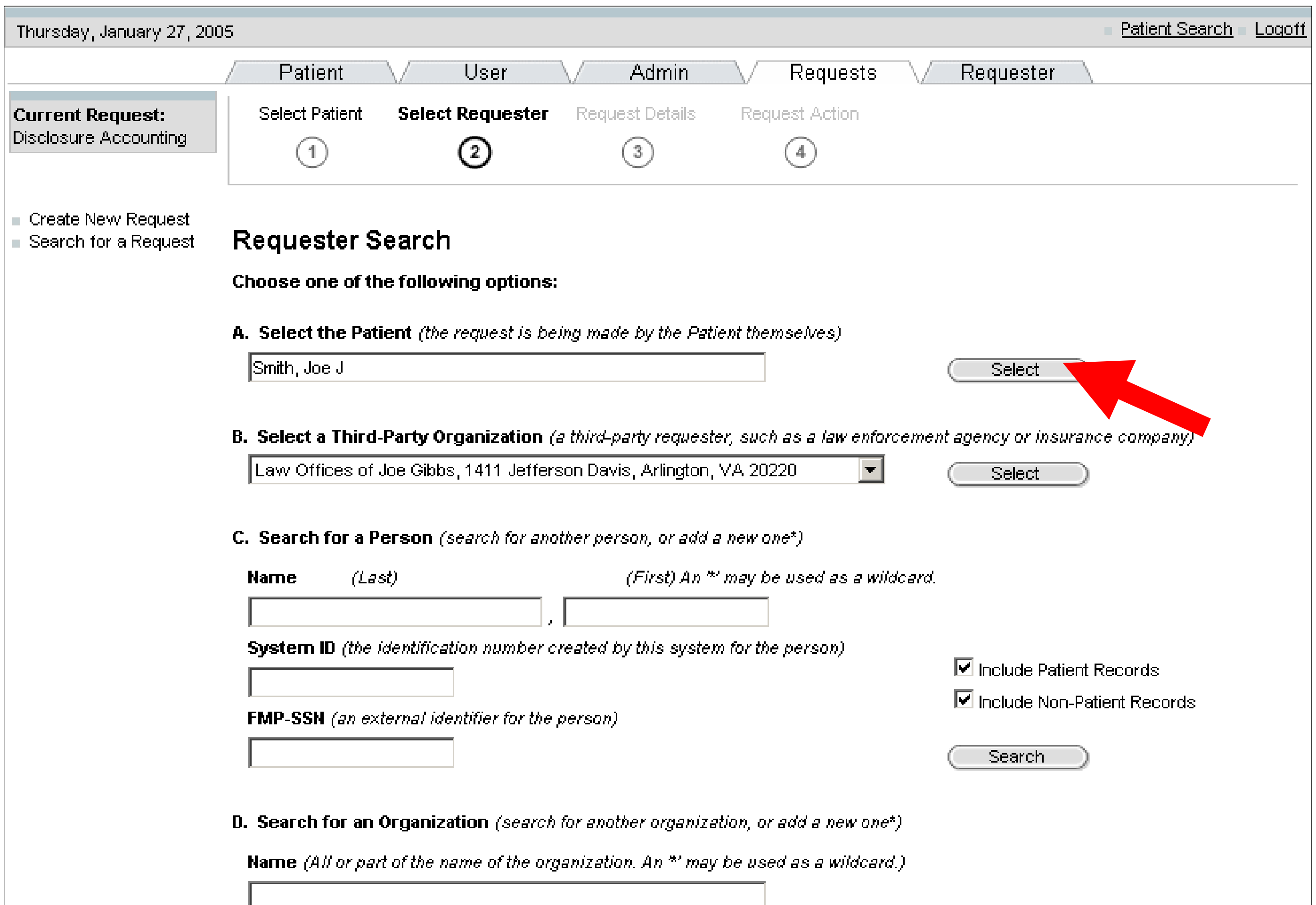
4. Search for or select the patient
5. Click on the OK button



Accounting of Disclosures

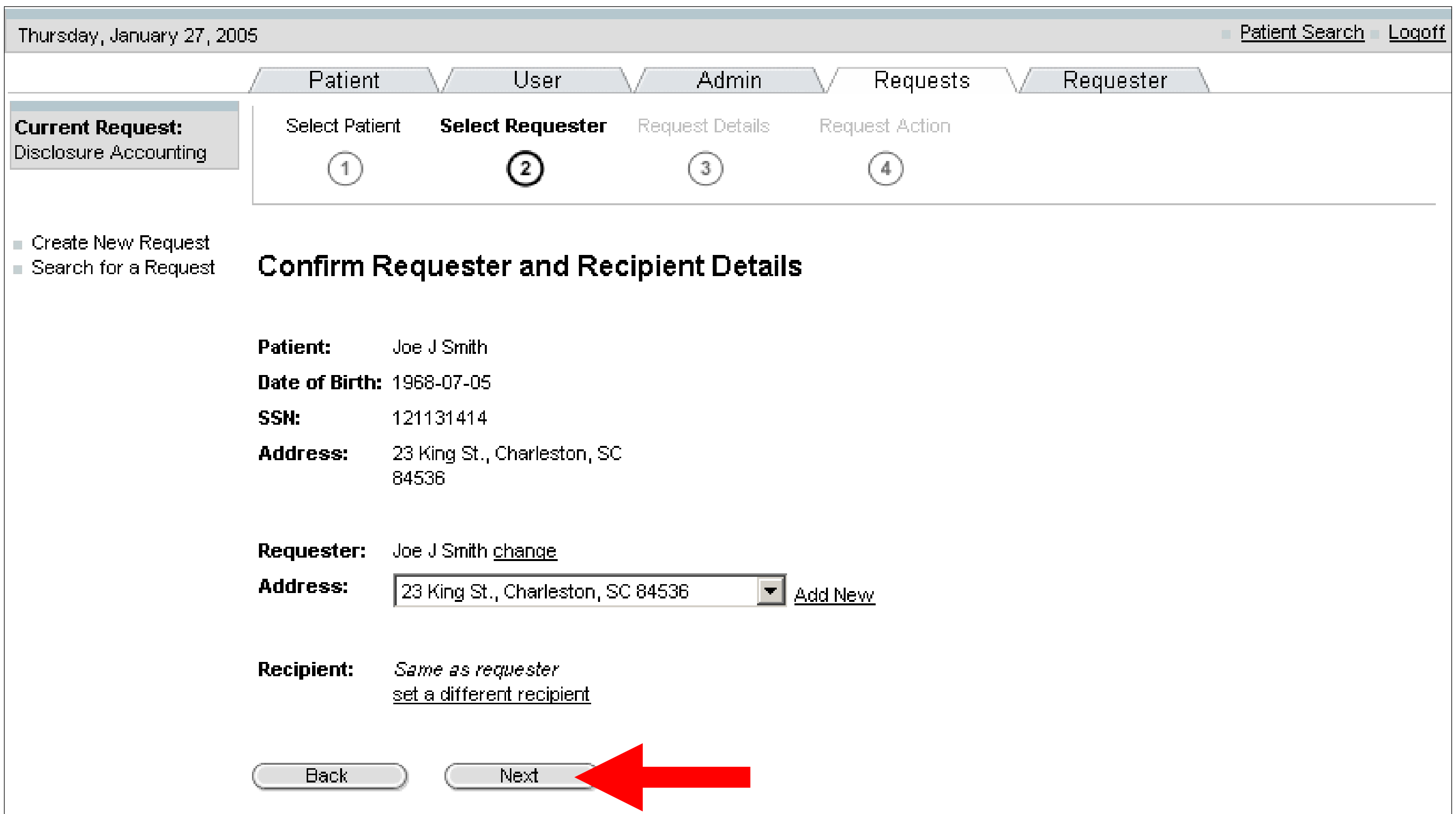
Recording a Request (4 of 9)

6. Select the requester (patient is requesting an accounting of disclosures)



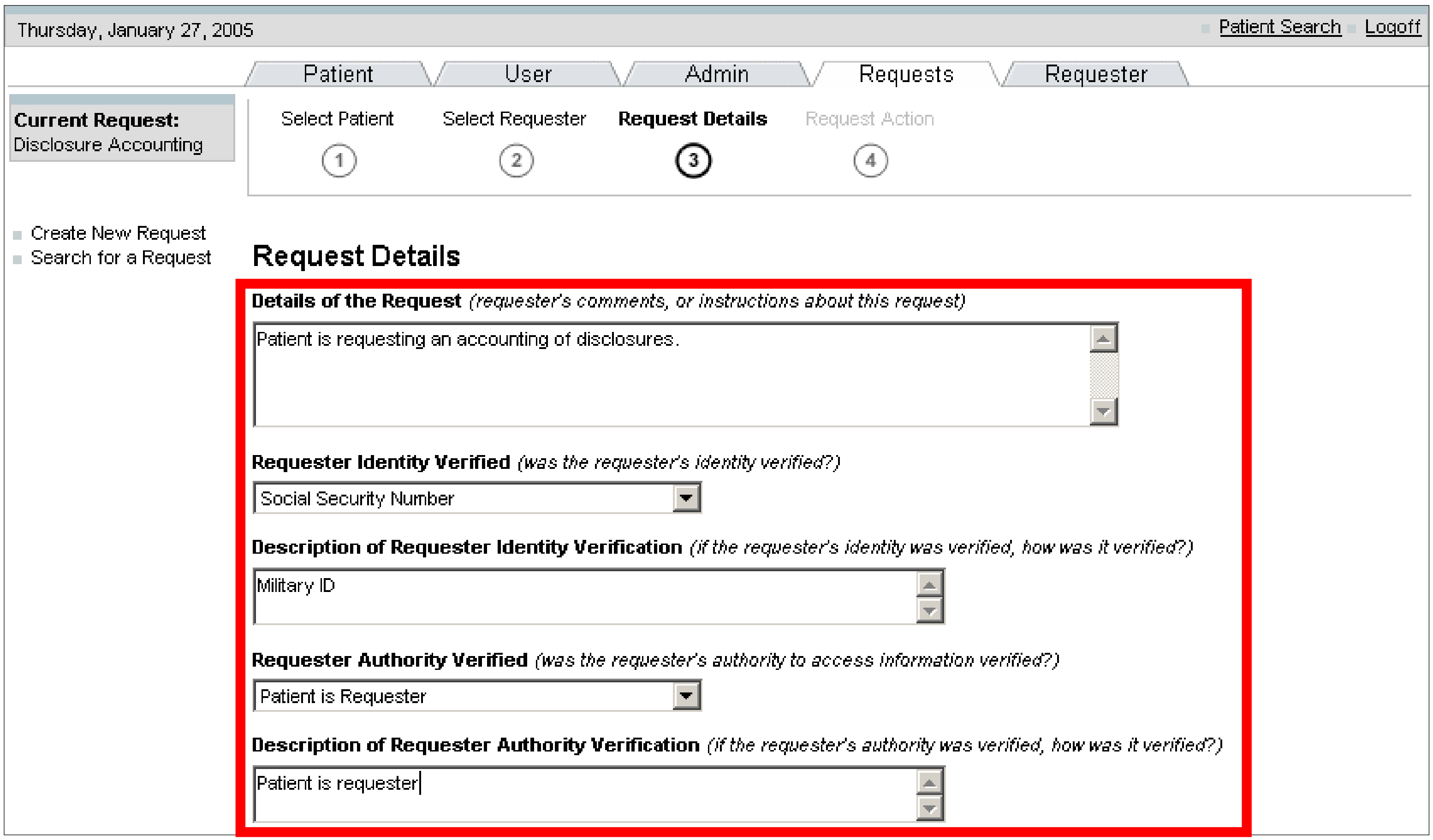
Recording a Request (5 of 9)

7. Confirm requester and recipient details (patient is requester)
8. Click on the Next button



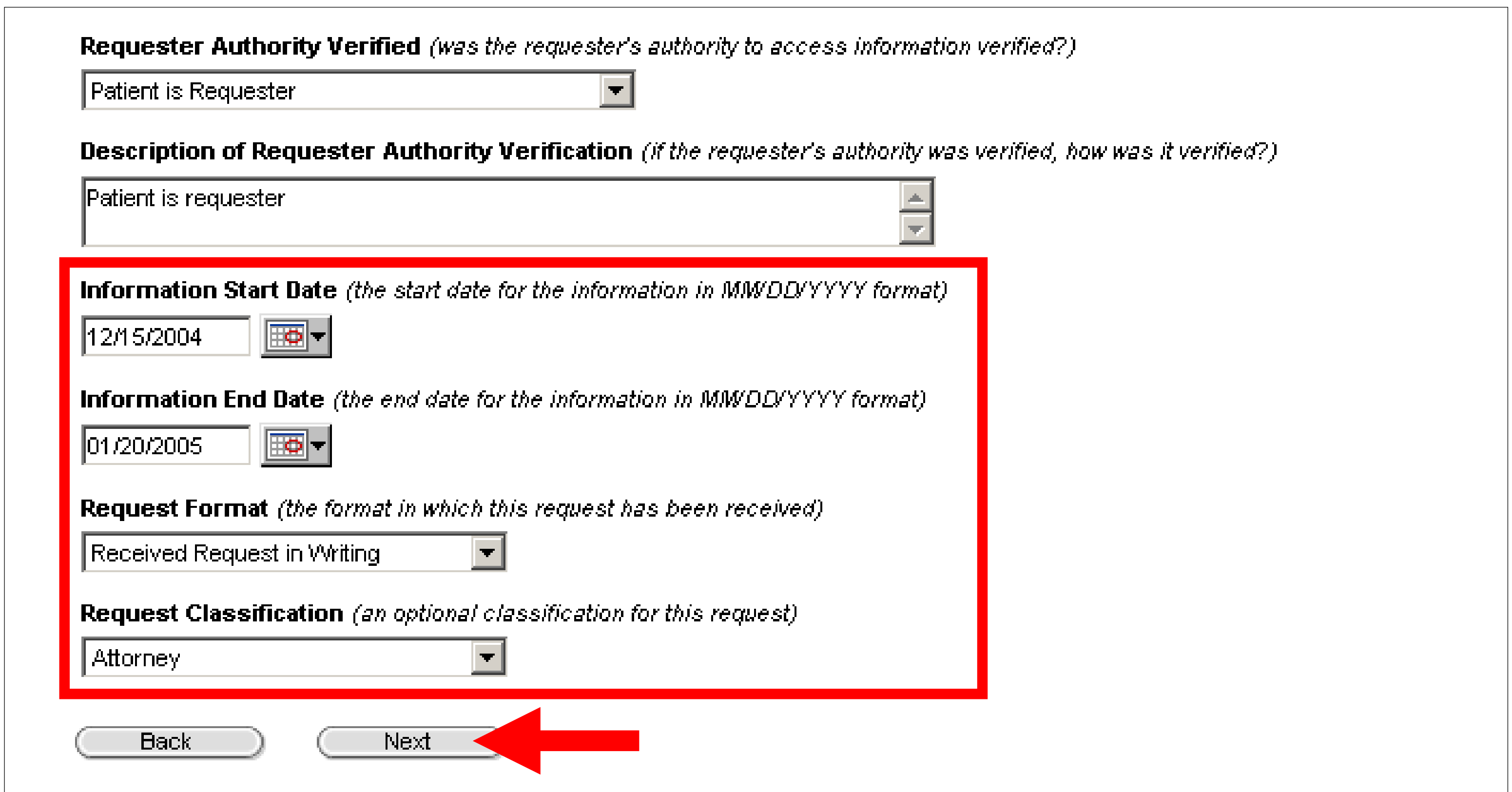
Recording a Request (6 of 9)

9. Enter the Request Details: (details of the request, identity verification, authority verification)



Recording a Request (7 of 9)

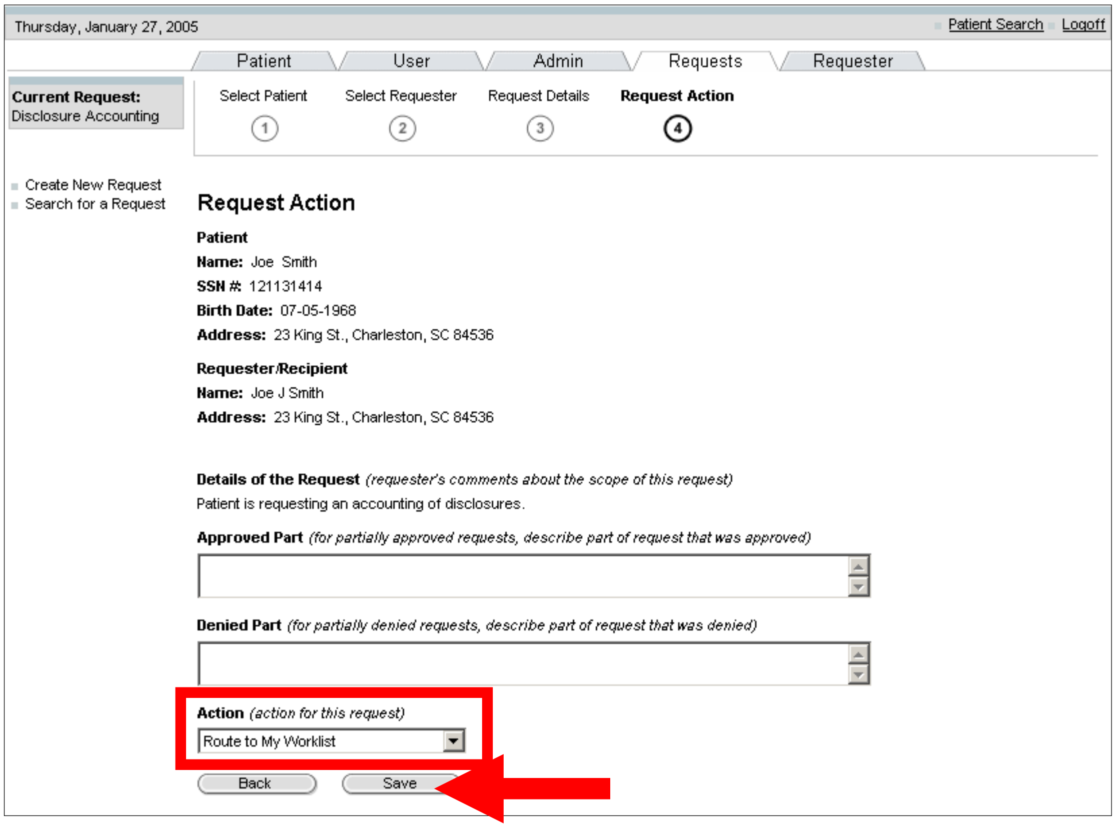
10. Scroll down the screen and enter: (Information start and end date, request format, and request classification)
11. Click on the Next button



Accounting of Disclosures

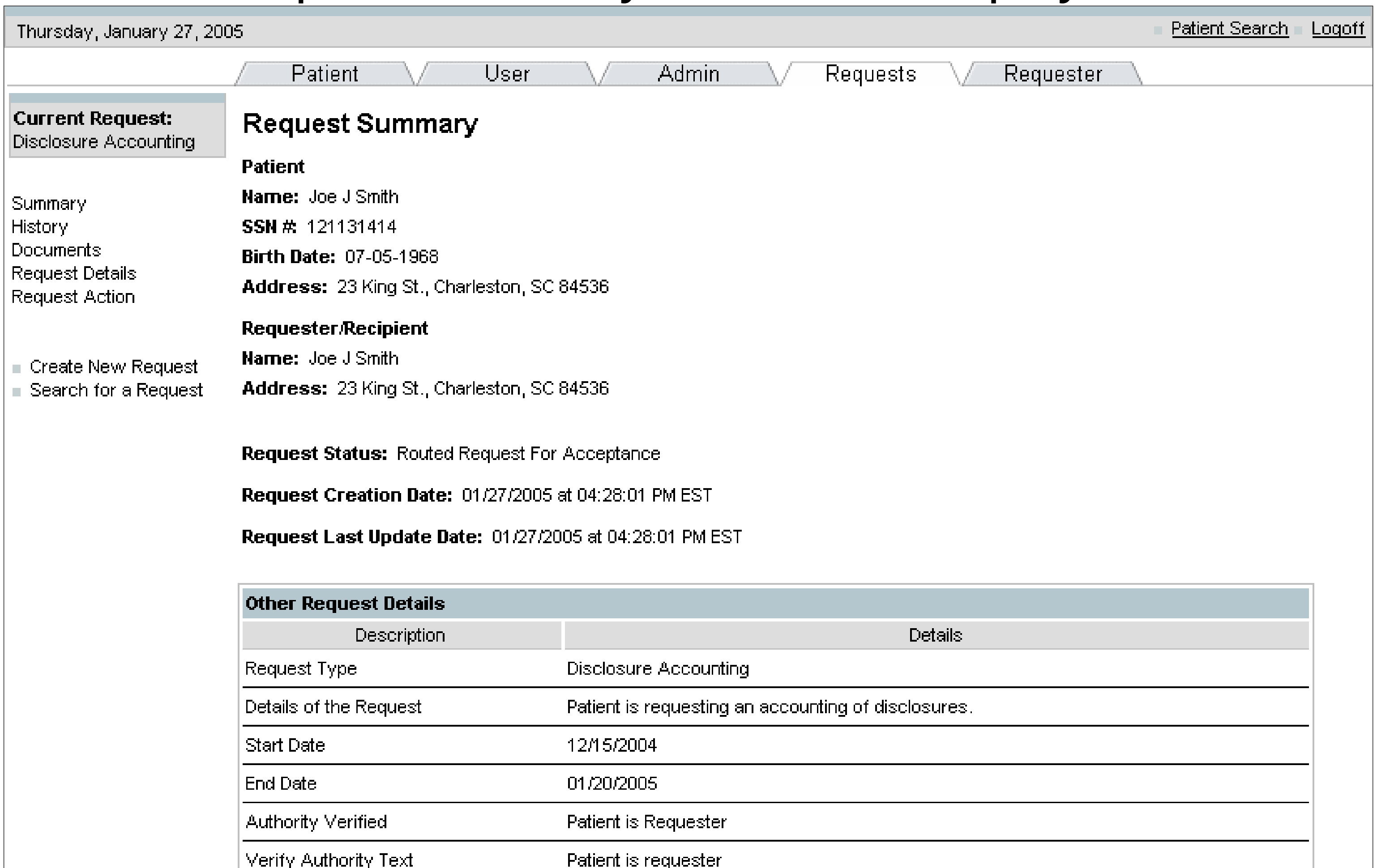
Recording a Request (8 of 9)

12. Enter in the Request Action details
13. From the Action drop-down box, select the appropriate person to route the request to
14. Click on the Save button



Recording a Request (9 of 9)

- The Request Summary screen will display



Thursday, January 27, 2005 Patient Search Logoff

Patient | User | Admin | Requests | Requester

Current Request:
Disclosure Accounting

Summary
History
Documents
Request Details
Request Action

- Create New Request
- Search for a Request

Request Summary

Patient

Name: Joe J Smith

SSN #: 121131414

Birth Date: 07-05-1968

Address: 23 King St., Charleston, SC 84536

Requester/Recipient

Name: Joe J Smith

Address: 23 King St., Charleston, SC 84536

Request Status: Routed Request For Acceptance

Request Creation Date: 01/27/2005 at 04:28:01 PM EST

Request Last Update Date: 01/27/2005 at 04:28:01 PM EST

Other Request Details

Description	Details
Request Type	Disclosure Accounting
Details of the Request	Patient is requesting an accounting of disclosures.
Start Date	12/15/2004
End Date	01/20/2005
Authority Verified	Patient is Requester
Verify Authority Text	Patient is requester

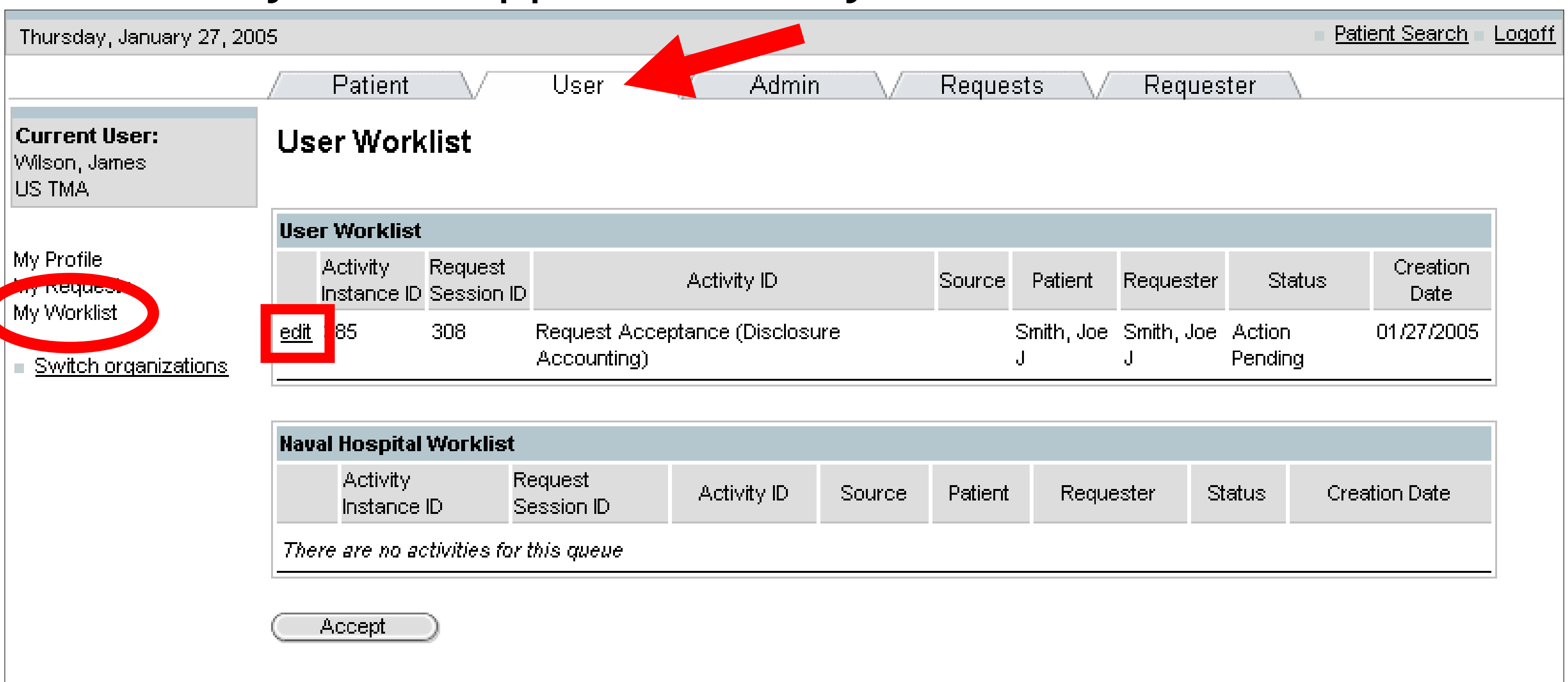
Approving/Denying a Request (1 of 4)

- Once a request for an accounting of disclosures has been recorded, a Privacy Specialist must approve or deny the request
- Once routed, the request will display in the Privacy Specialist's work list

Accounting of Disclosures

Approving/Denying a Request (2 of 4)

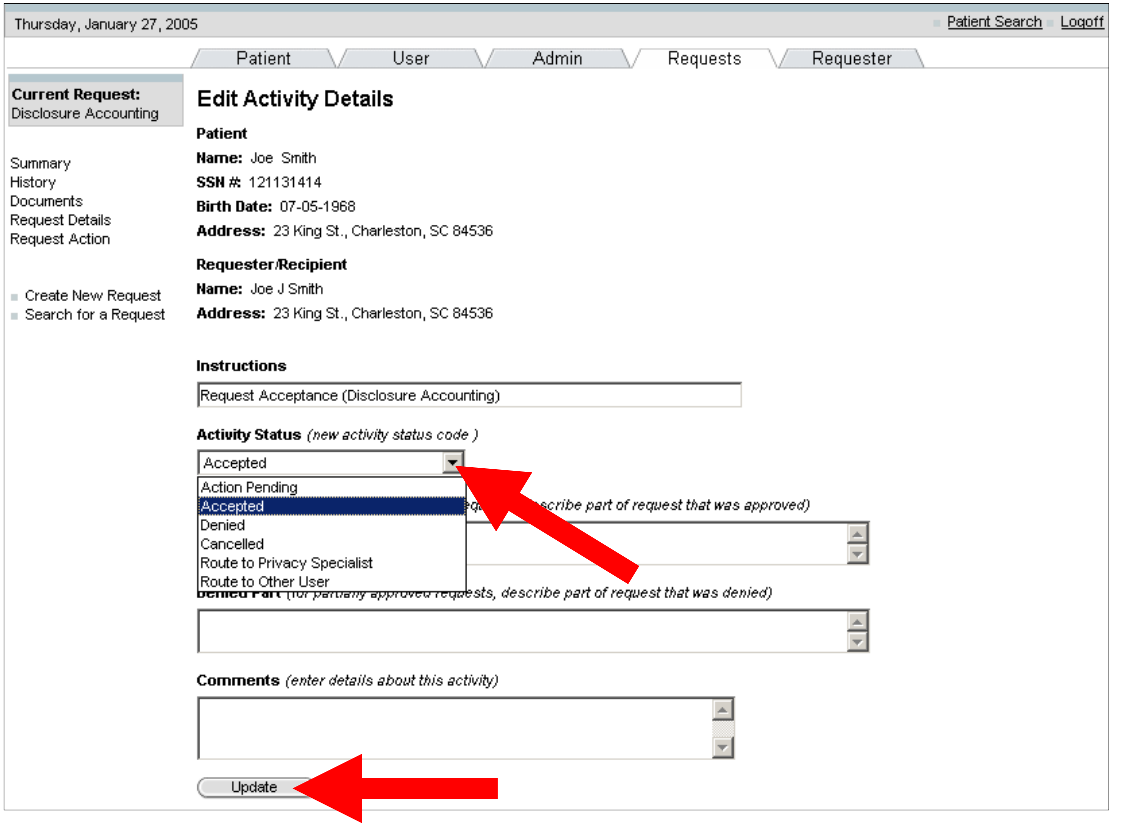
1. Select the User tab
2. Select My Worklist hyperlink
3. Select the Edit hyperlink for that disclosure accounting that you will approve or deny



Approving/Denying a Request (3 of 4)

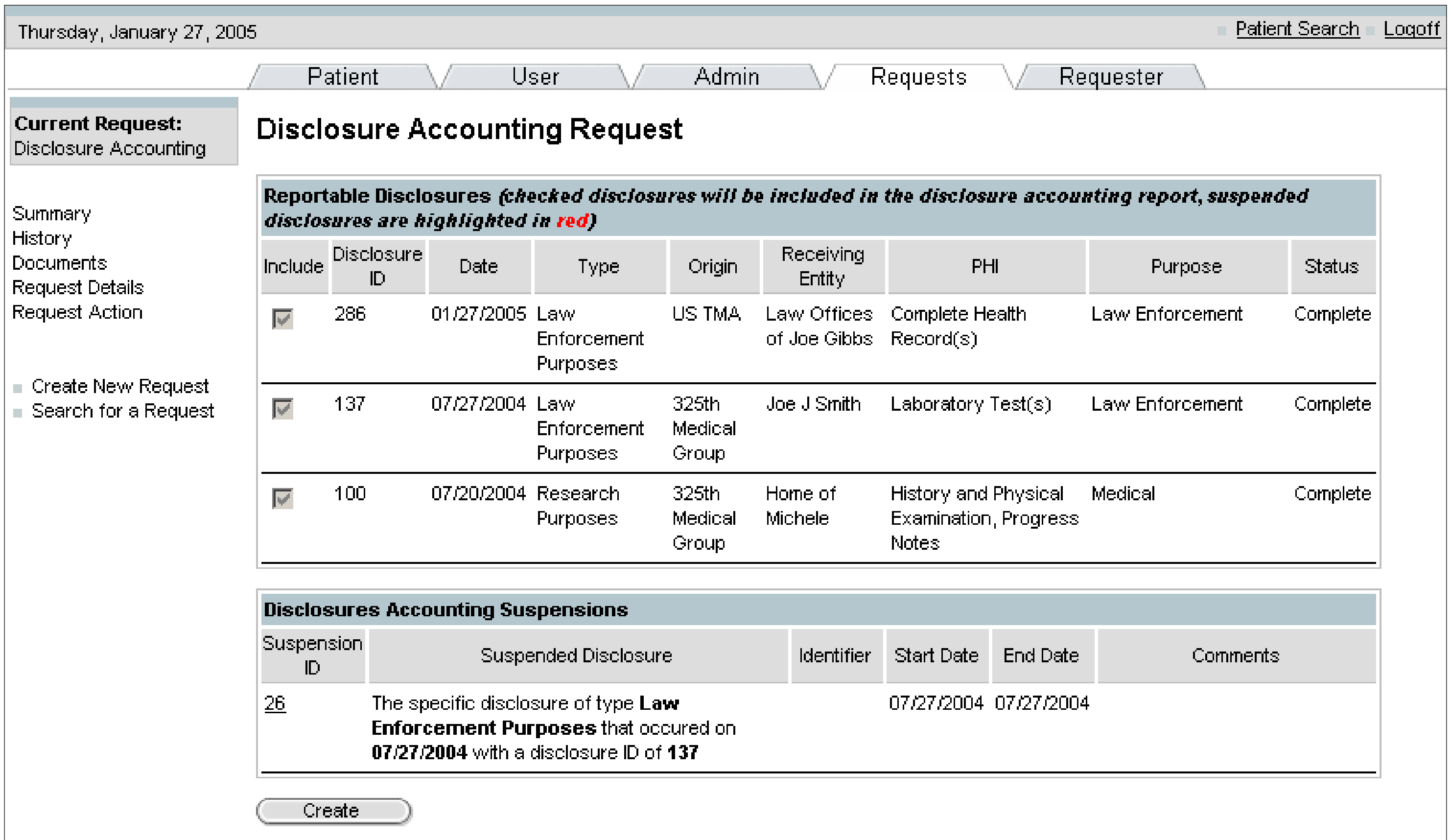
- The Edit Activity Details screen will display

4. Select Accepted or Denied from the Activity Status drop-down box
5. Click on the Update button



Approving/Denying a Request (4 of 4)

- The Disclosure Accounting Request screen will display with the approved accounting of disclosures



Thursday, January 27, 2005 — Patient Search | Logoff

Patient | User | Admin | Requests | Requester

Current Request:
Disclosure Accounting

Summary
History
Documents
Request Details
Request Action

- Create New Request
- Search for a Request

Disclosure Accounting Request

Reportable Disclosures ***(checked disclosures will be included in the disclosure accounting report, suspended disclosures are highlighted in red)***

Include	Disclosure ID	Date	Type	Origin	Receiving Entity	PHI	Purpose	Status
☑	286	01/27/2005	Law Enforcement Purposes	US TMA	Law Offices of Joe Gibbs	Complete Health Record(s)	Law Enforcement	Complete
☑	137	07/27/2004	Law Enforcement Purposes	325th Medical Group	Joe J Smith	Laboratory Test(s)	Law Enforcement	Complete
☑	100	07/20/2004	Research Purposes	325th Medical Group	Home of Michele	History and Physical Examination, Progress Notes	Medical	Complete

Disclosures Accounting Suspensions

Suspension ID	Suspended Disclosure	Identifier	Start Date	End Date	Comments
26	The specific disclosure of type **Law Enforcement Purposes** that occured on **07/27/2004** with a disclosure ID of **137**		07/27/2004	07/27/2004	

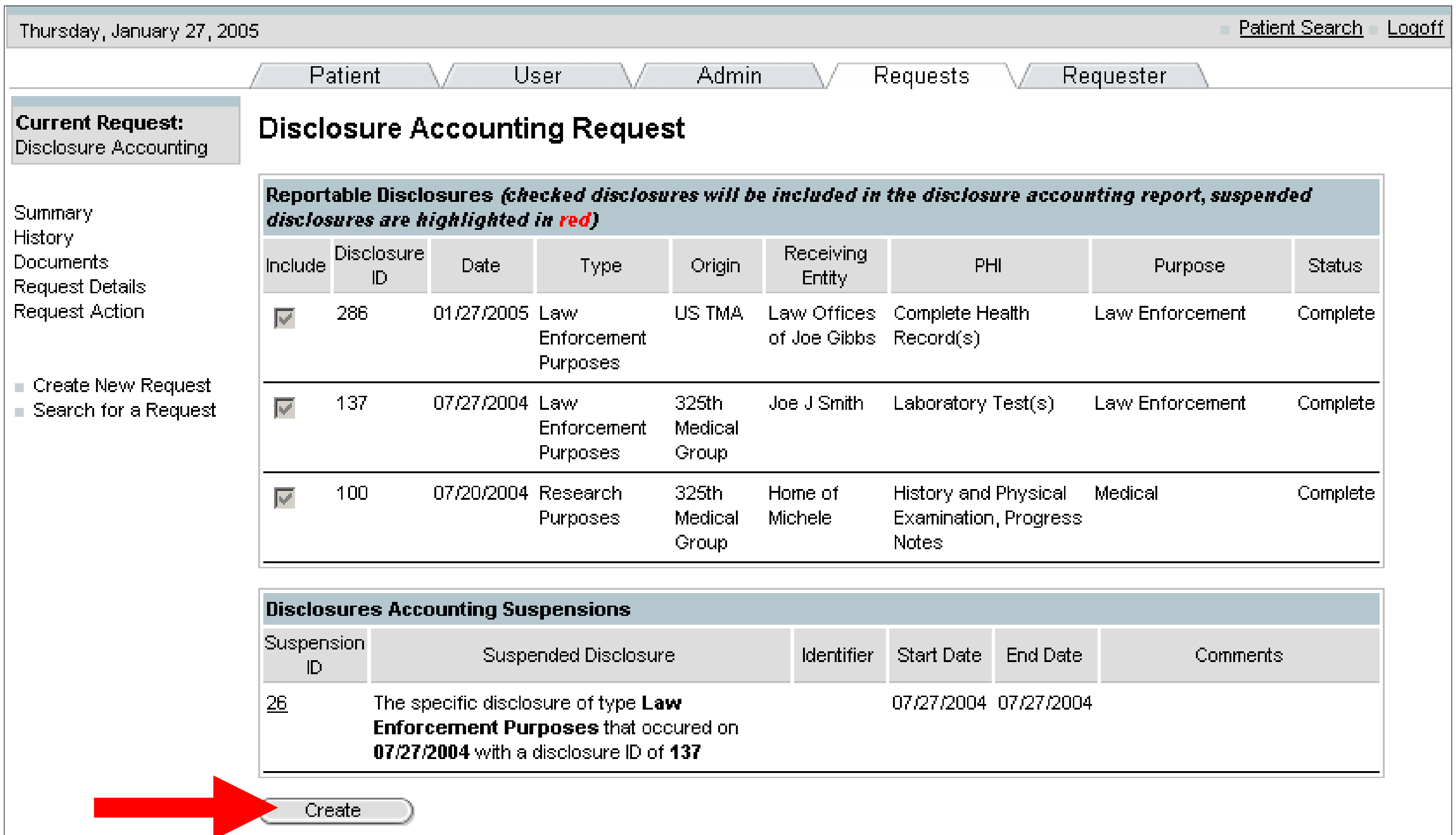
Create

Generating an Accounting of Disclosures Report (1 of 4)

- An accounting of disclosures report is a summary of all of the disclosures made for a particular patient
  - Pending disclosures will not display in the report
- Once a request has been approved, an accounting of disclosures report can be generated
- The Privacy Specialist has the option to route the report back to the originator

Generating an Accounting of Disclosures Report (2 of 4)

1. From the Disclosure Accounting Request screen, click on the Create button to generate the report



Thursday, January 27, 2005 — Patient Search Logoff

Patient | User | Admin | Requests | Requester

Current Request:
Disclosure Accounting

Summary
History
Documents
Request Details
Request Action

- Create New Request
- Search for a Request

Disclosure Accounting Request

Reportable Disclosures ***(checked disclosures will be included in the disclosure accounting report, suspended disclosures are highlighted in red)***

Include	Disclosure ID	Date	Type	Origin	Receiving Entity	PHI	Purpose	Status
☑	286	01/27/2005	Law Enforcement Purposes	US TMA	Law Offices of Joe Gibbs	Complete Health Record(s)	Law Enforcement	Complete
☑	137	07/27/2004	Law Enforcement Purposes	325th Medical Group	Joe J Smith	Laboratory Test(s)	Law Enforcement	Complete
☑	100	07/20/2004	Research Purposes	325th Medical Group	Home of Michele	History and Physical Examination, Progress Notes	Medical	Complete

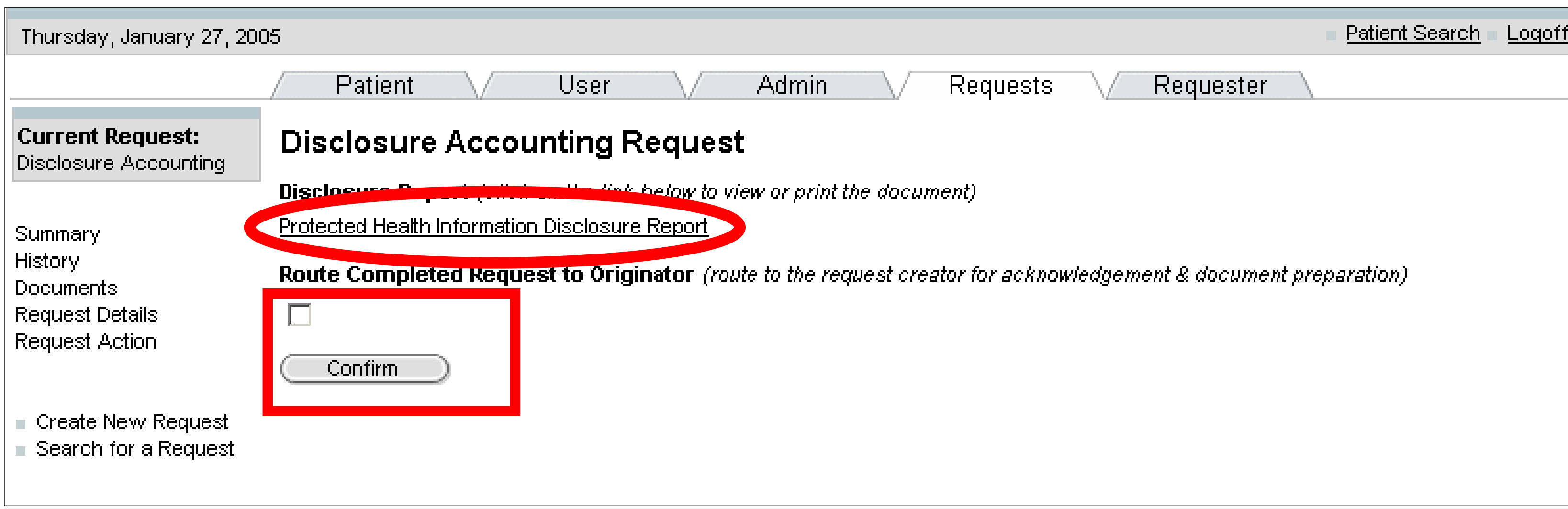
Disclosures Accounting Suspensions

Suspension ID	Suspended Disclosure	Identifier	Start Date	End Date	Comments
26	The specific disclosure of type **Law Enforcement Purposes** that occured on **07/27/2004** with a disclosure ID of **137**		07/27/2004	07/27/2004	

Create

Generating an Accounting of Disclosures Report (3 of 4)

2. Select the Protected Health Information Disclosure Report hyperlink to create the report
3. If you want to route the completed request back to the originator, place a check in the box and click on Confirm



Accounting of Disclosures

Generating an Accounting of Disclosures Report (4 of 4)

- The Accounting of Disclosures Report will display

Protected Health Information Disclosure Report

Prepared for: Joe J Smith

Requested from: US TMA

Generated on: 01-27-2005

Disclosure ID:	286
Date:	2005-01-27
Disclosure Type:	Law Enforcement Purposes - Law Enforcement Purposes
Disclosure Purpose:	Law Enforcement
Disclosed Health Information:	Complete Health Record(s)
Disclosure Originated From:	US TMA Five Skyline Place, 5111 Leesburg Pike, Falls Church, VA 22041-3206
Disclosure Recipient:	Law Offices of Joe Gibbs 1411 Jefferson Davis, Arlington, VA 20220
Disclosure Requester:	Smith, Joe J 23 King St., Charleston, SC 84536

Disclosure ID:	137

Summary

- You should now be able to:
  - Record a request for an accounting of disclosures
  - Approve/deny a request for an accounting of disclosures
  - Generate an accounting of disclosures report

Accounting Suspensions

Objectives

- Upon completion of this lesson, you will be able to:
  - Create an accounting suspension

Creating a Suspension (1 of 7)

- The covered entity shall temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official…DoD 6025.18-R C13.1.2.1
- Two types of disclosures can be suspended:
  - Law enforcement purposes
  - Health oversight activities
- Privacy Specialists have the ability to enter an accounting suspension in two ways
  - Specific disclosure
  - Type of disclosure
- Once entered, the suspension can be viewed by all users

Accounting Suspensions

Creating a Suspension (2 of 7)

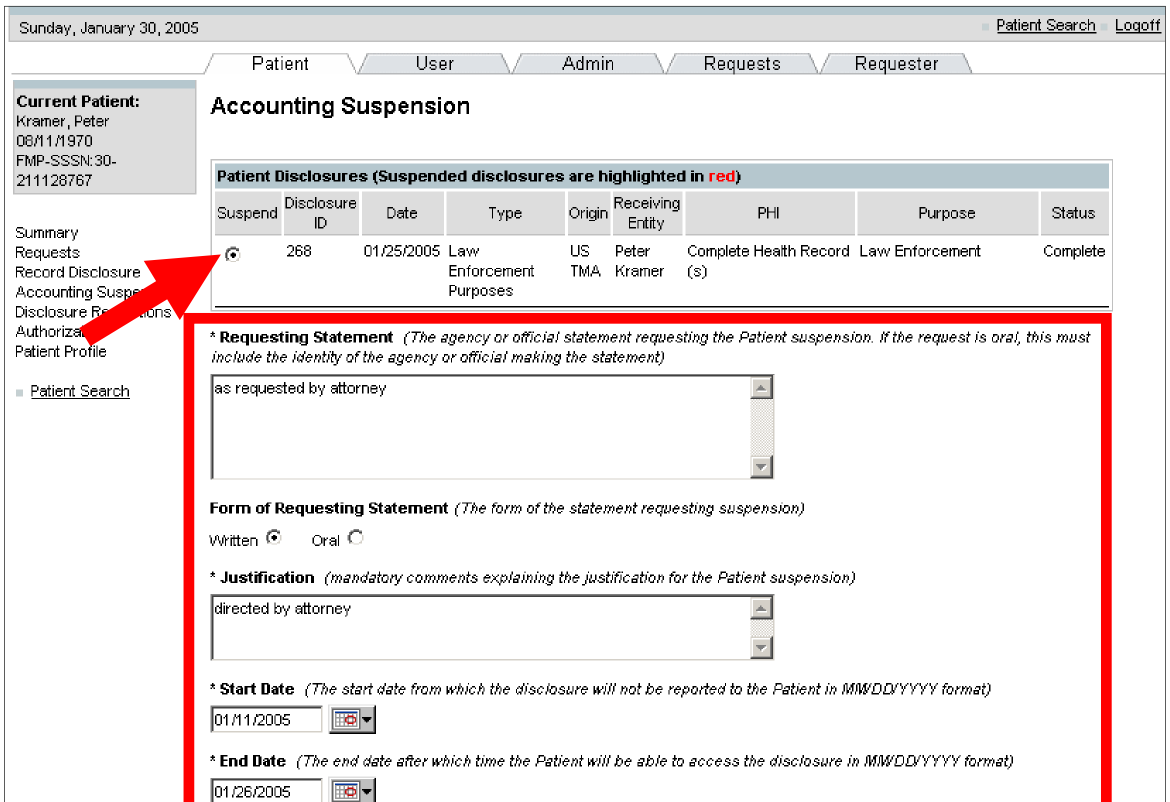
1. Search for and select a patient record
2. Select the Accounting Suspensions hyperlink

Creating a Suspension (3 of 7)

3. Select the Specific Disclosure hyperlink

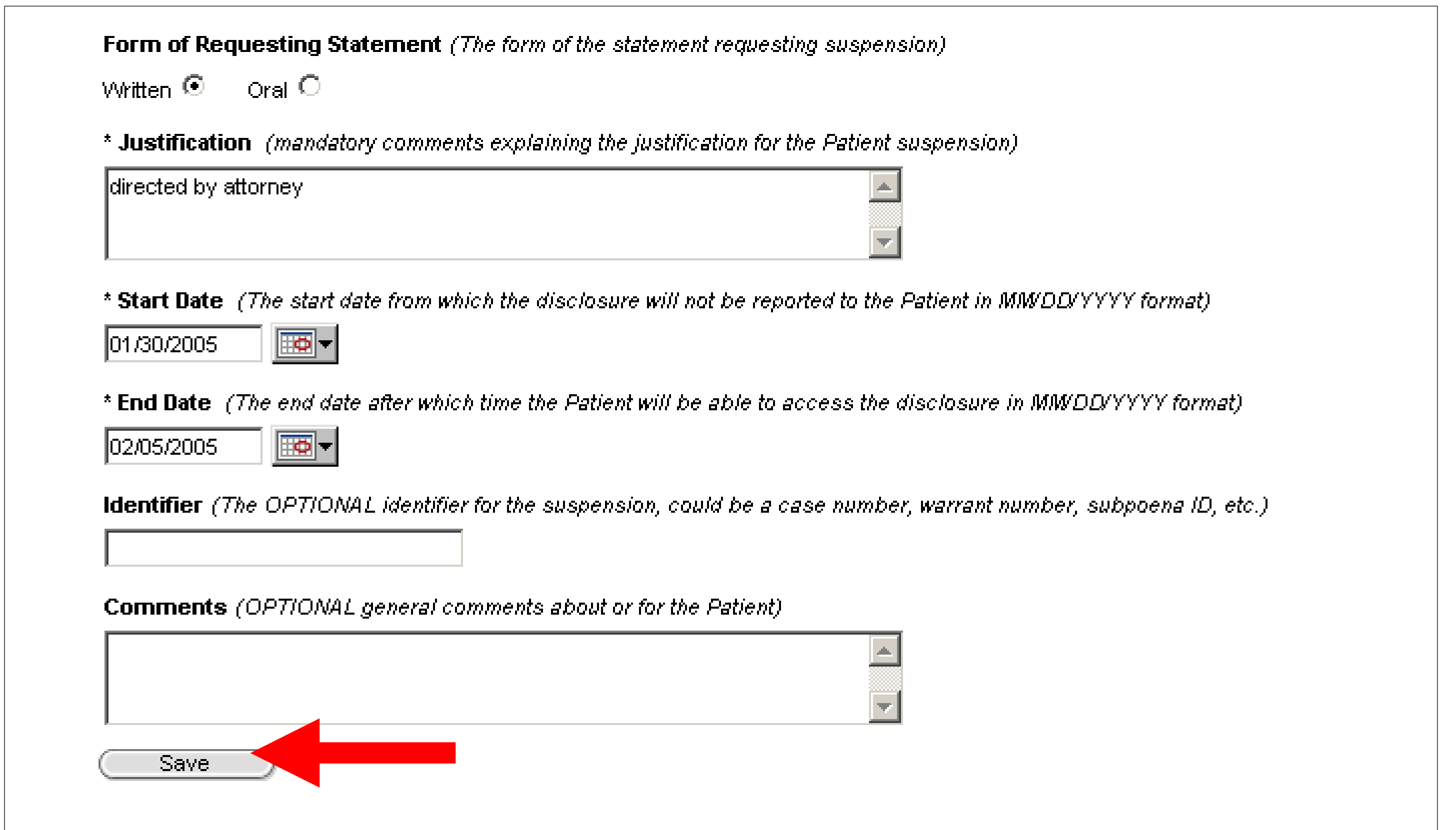
Creating a Suspension (4 of 7)

4. Click on the radio button for the disclosure you want to suspend
5. Enter the suspension details: (requesting statement and form, justification, and start and end date)



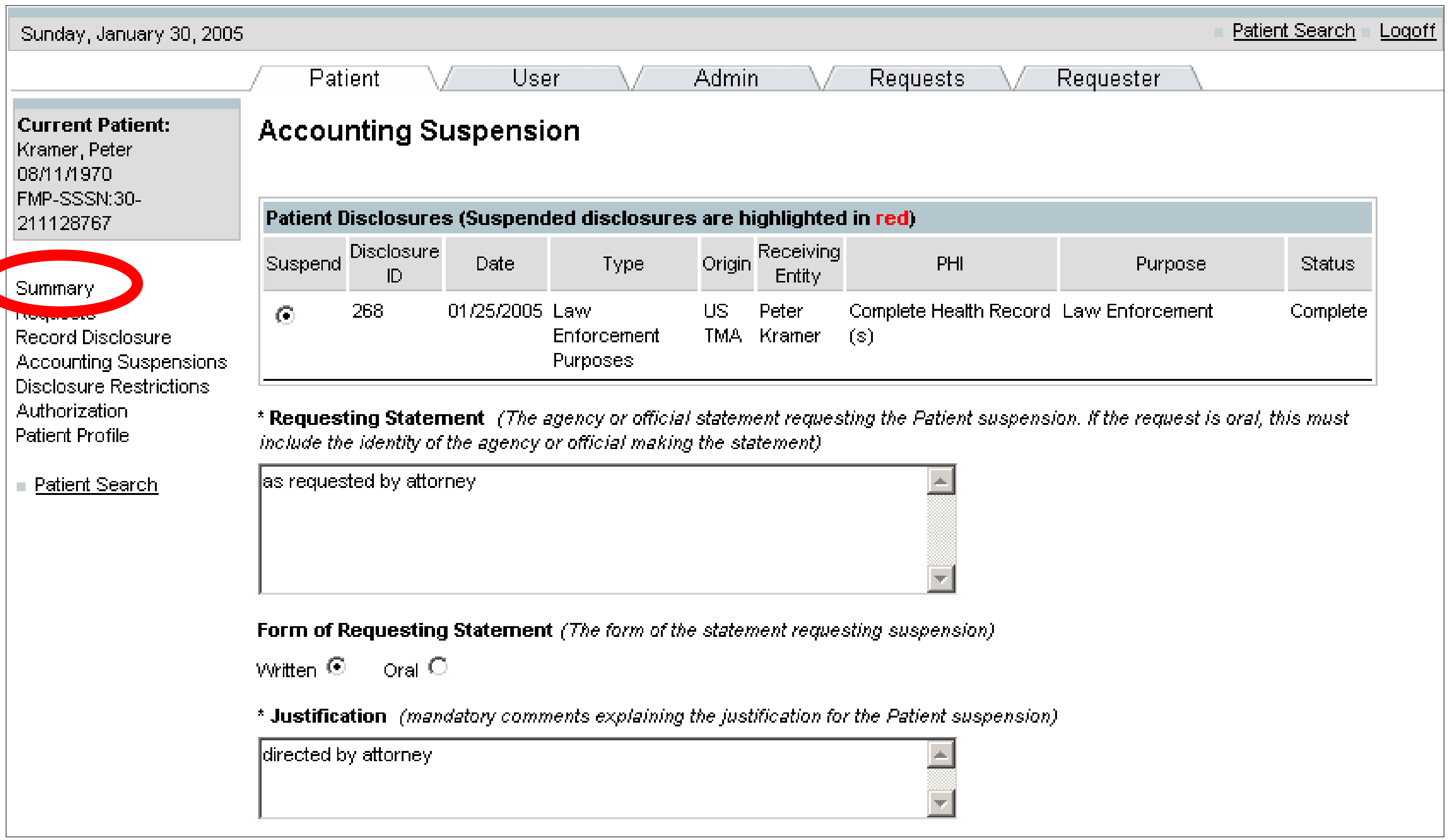
Creating a Suspension (5 of 7)

6. Scroll to the bottom of the screen and click the Save button



Creating a Suspension (6 of 7)

7. Select the Summary hyperlink

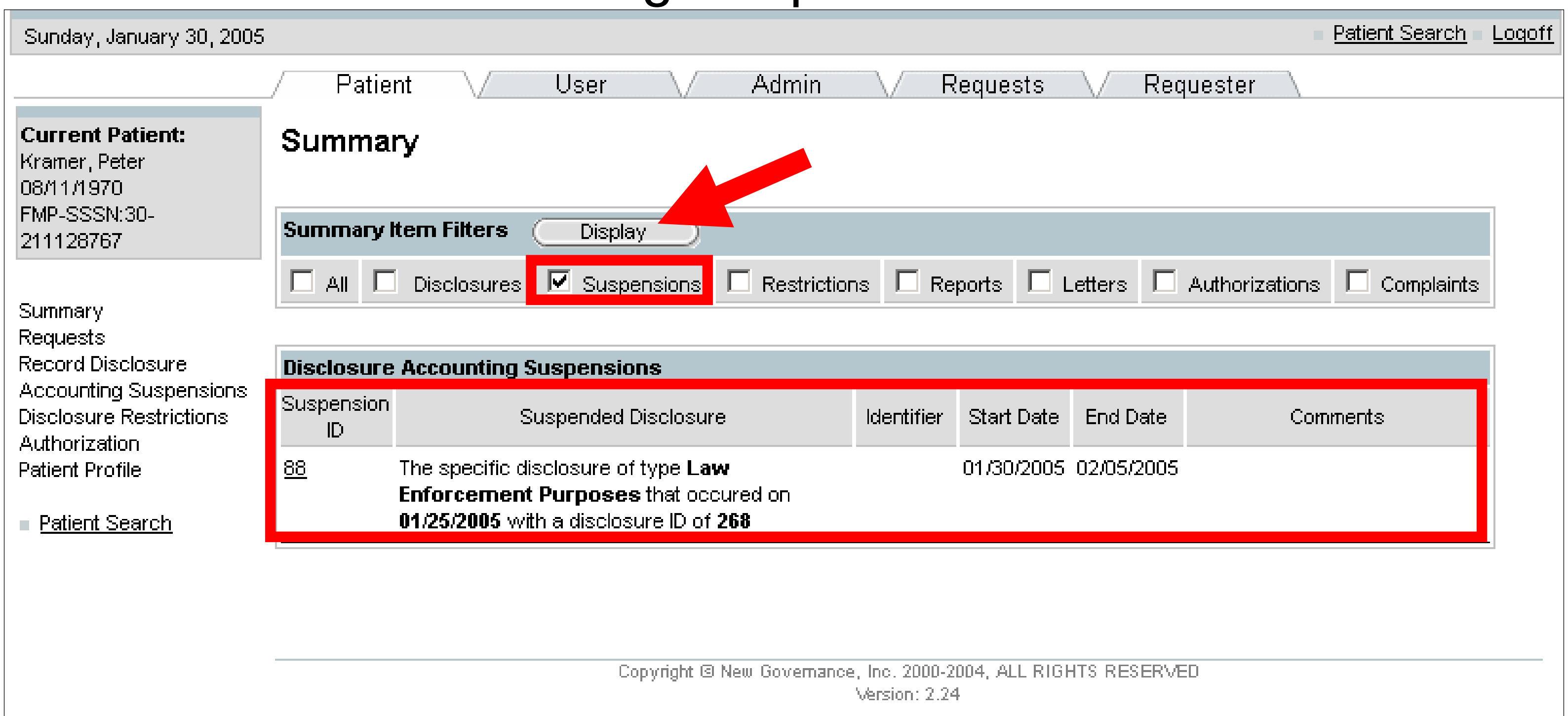


Accounting Suspensions

Creating a Suspension (7 of 7)

8. Check the Suspensions checkbox
9. Click on the Display button

- The Disclosure that you suspended will display in the Disclosure Accounting Suspensions section



Summary

- You should now be able to:
  - Create an accounting suspension

Disclosure Restrictions

Disclosure Restrictions

Objectives

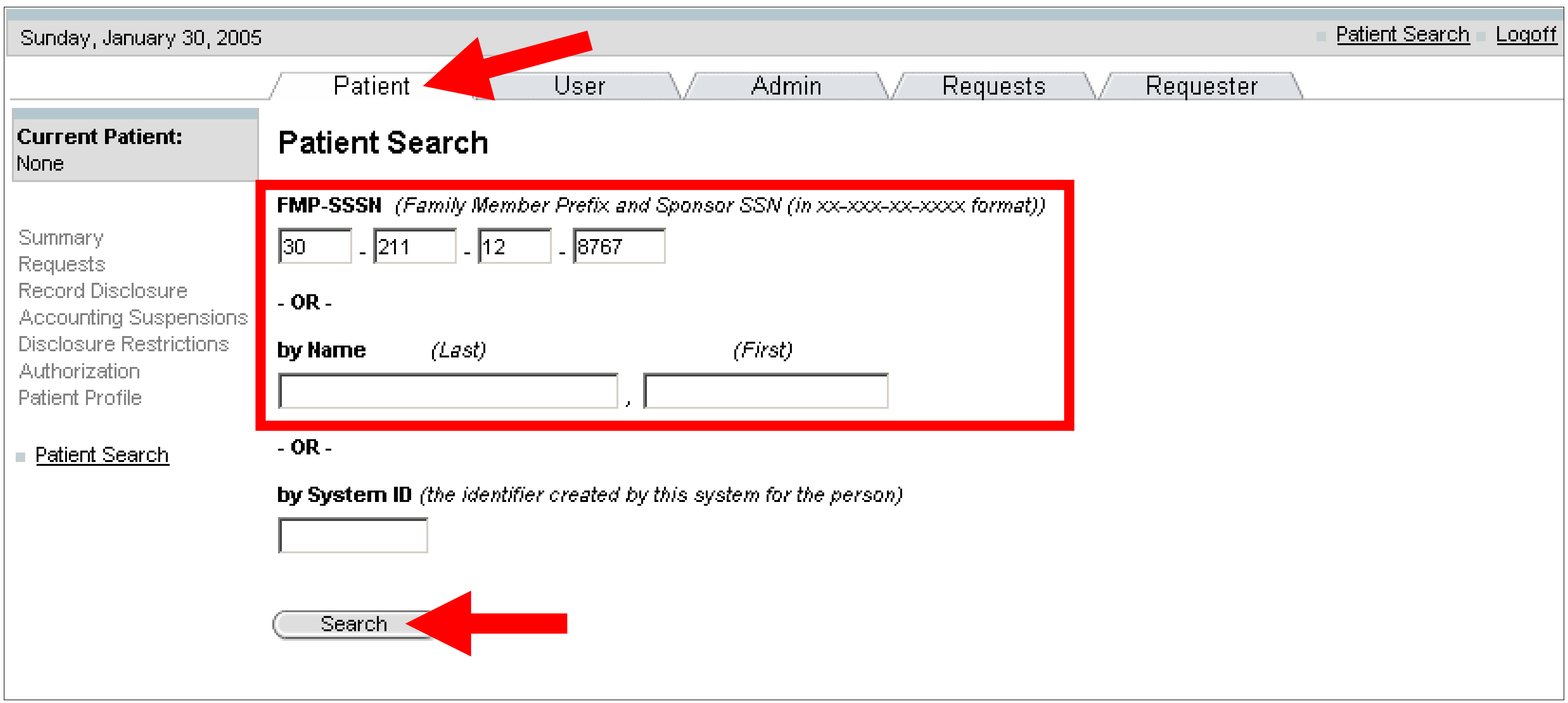
- Upon completion of this lesson, you will be able to:
  - Record a disclosure restriction request
  - Approve or deny the disclosure restriction request
  - Generate an approval or denial letter to be sent to the requester

Recording a Restriction (1 of 6)

- DoD 6025.18-R Chapter 10 describes the rights to request privacy protection for protected health information
  - Covered entity is not required to agree to such requests
  - Requests may be made orally or in writing, but must be documented
  - Covered entity must provide a response to the individual
- Privacy Specialists can record and approve or deny requests for disclosure restrictions
  - Once approved or denied, a letter with an explanation can be generated

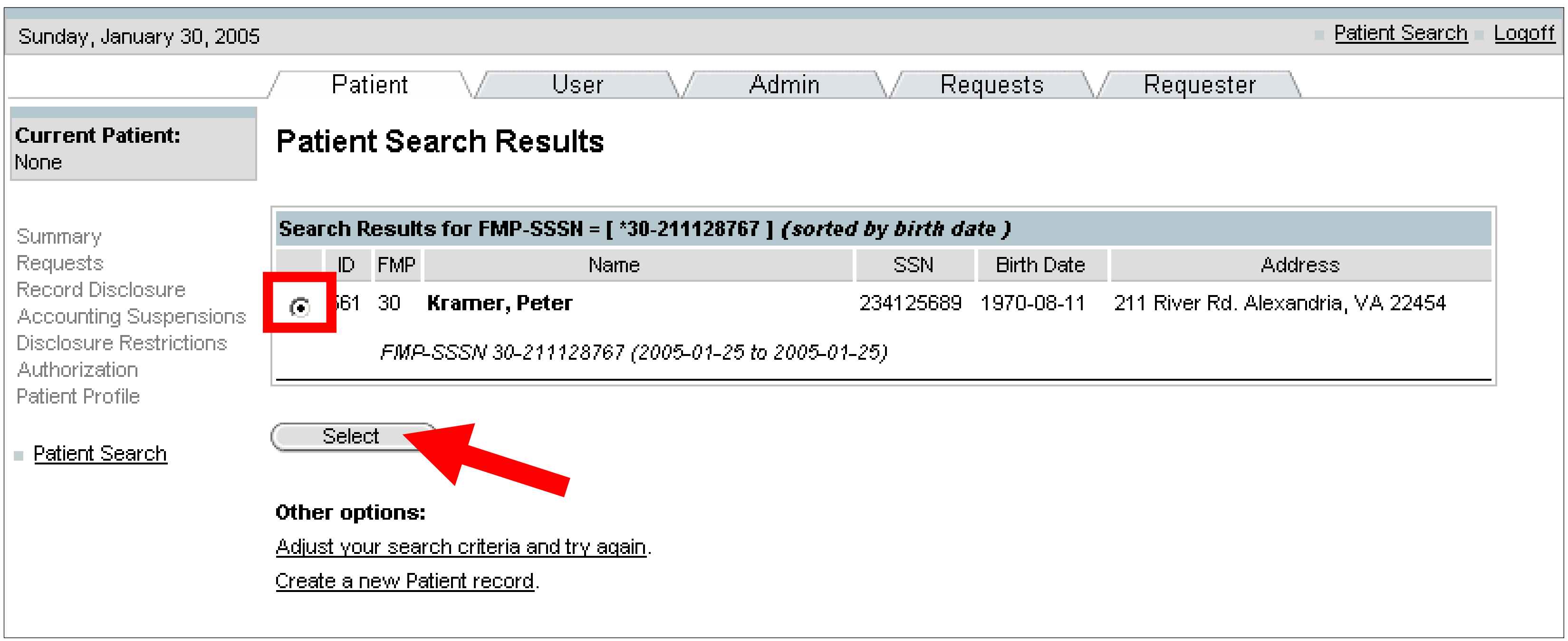
Recording a Restriction (2 of 6)

1. Select the Patient tab
2. Enter patient search criteria
3. Click on Search



Recording a Restriction (3 of 6)

4. Click on the radio button for the patient
5. Click on the Select button



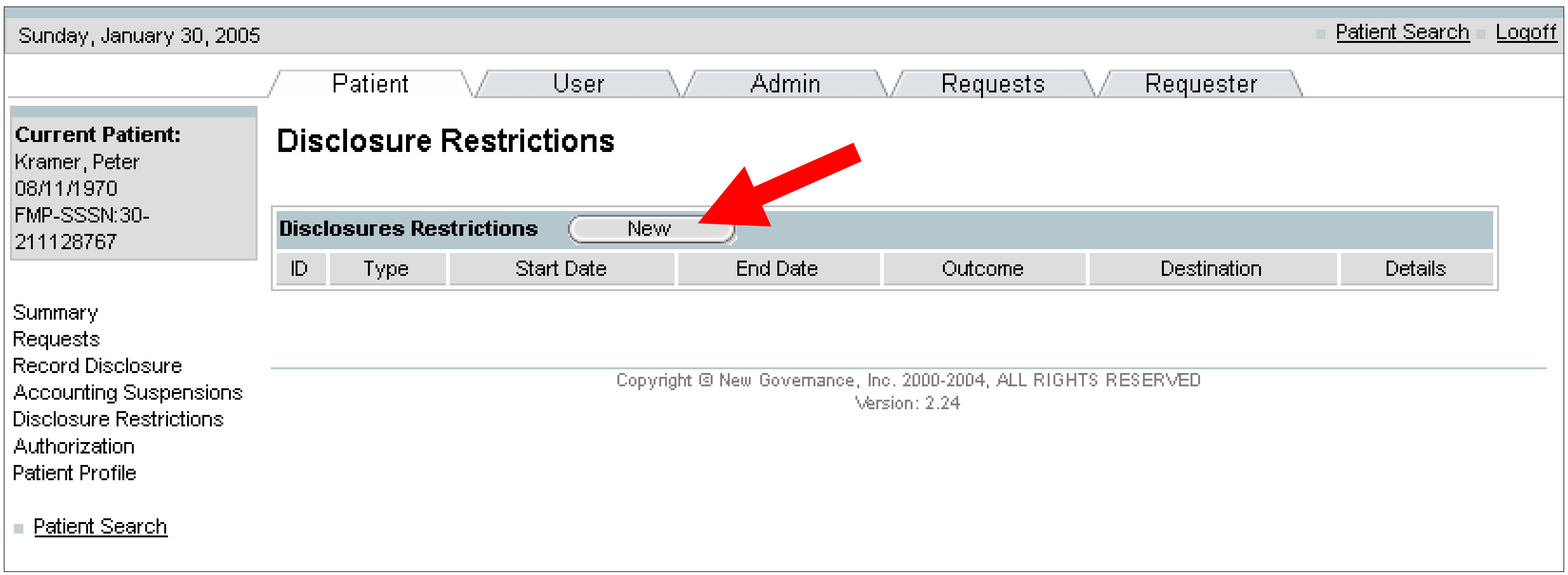
Recording a Restriction (4 of 6)

6. Select the Disclosure Restrictions hyperlink

Disclosure Restrictions

Recording a Restriction (5 of 6)

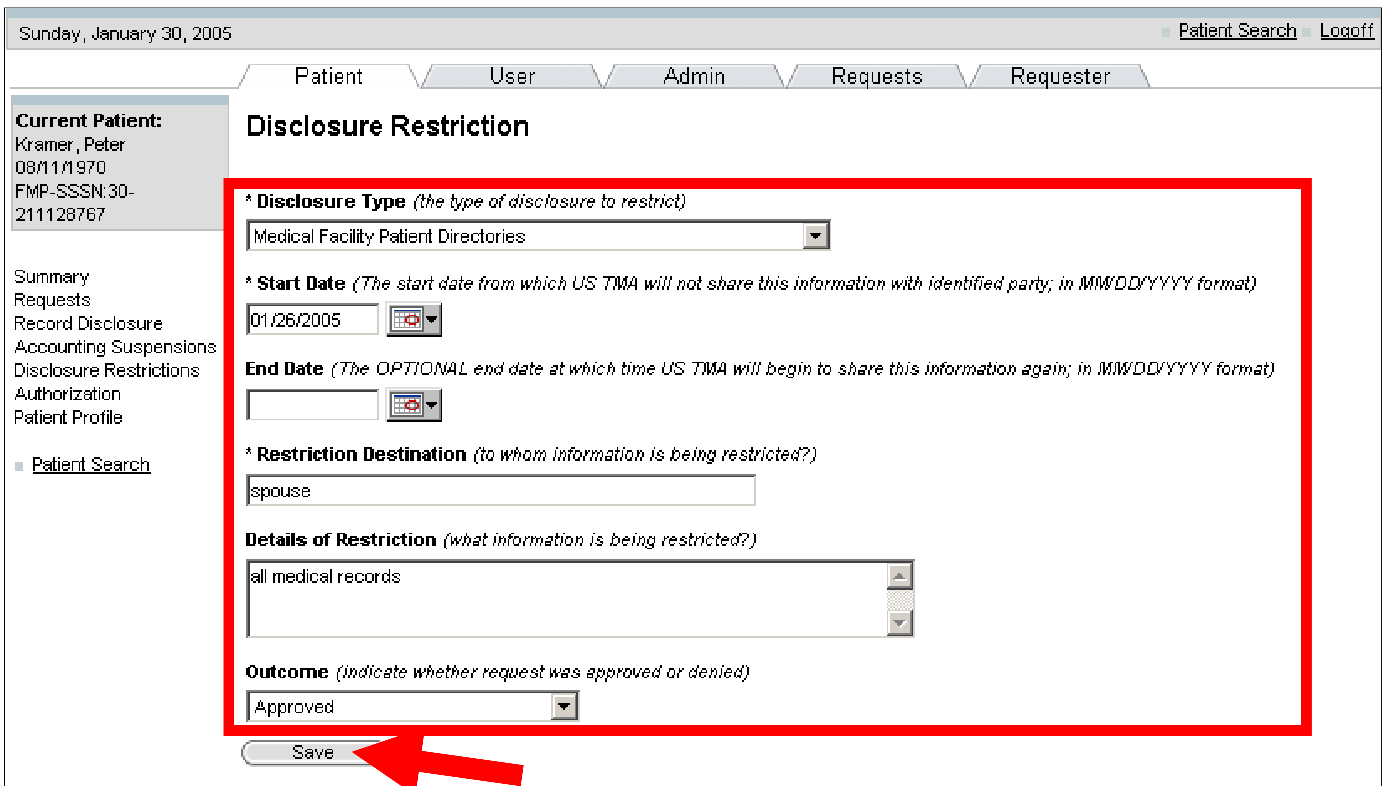
7. Click on the New button in the Disclosure Restrictions box



Disclosure Restrictions

Recording a Restriction (6 of 6)

8. Enter Disclosure Restriction details: (Disclosure type, start and end date, destination, and details)
9. Select Approved or Denied from the Outcome drop-down box
10. Click on the Save button



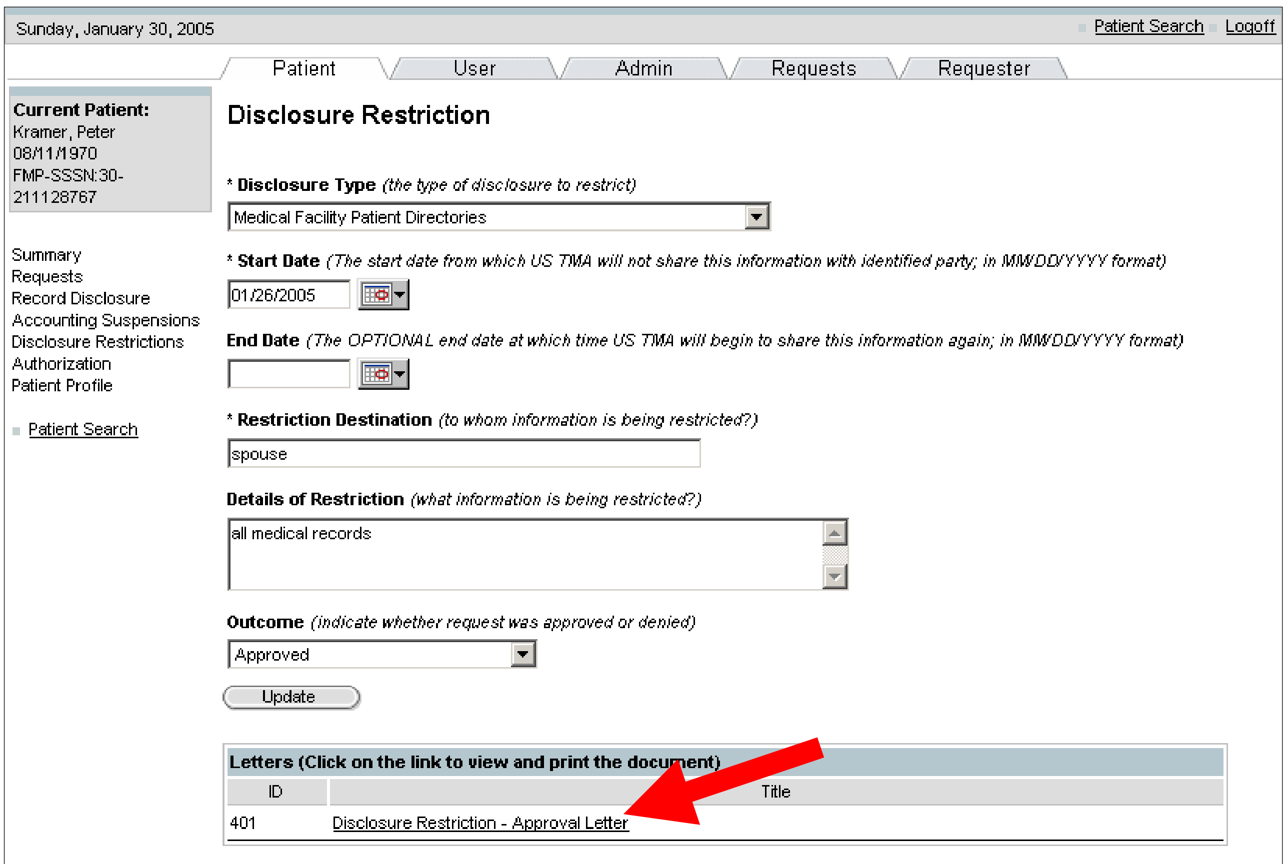
Generating Correspondence (1 of 3)

- Once you have approved or denied the disclosure restriction you have the ability to generate an approval or denial letter
- The letter will be pre-populated with the information that you entered for that particular restriction

Generating Correspondence (2 of 3)

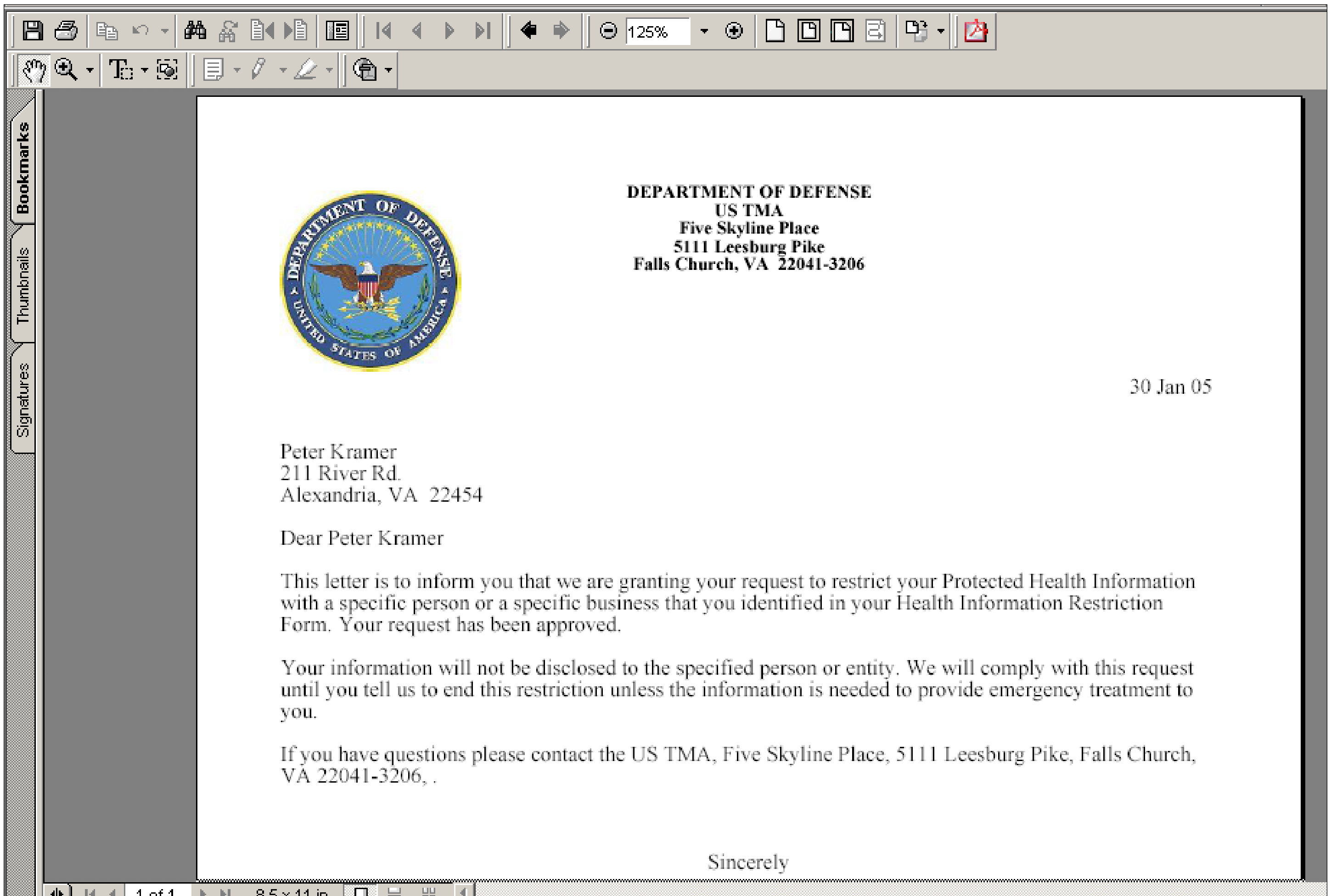
- Once you have clicked on the Save button, the letters box will appear

1. Select the Title hyperlink to access the letter



Generating Correspondence (3 of 3)

- The Approval letter is generated



DEPARTMENT OF DEFENSE
US TMA
Five Skyline Place
5111 Leesburg Pike
Falls Church, VA 22041-3206

30 Jan 05

Peter Kramer
211 River Rd.
Alexandria, VA 22454

Dear Peter Kramer

This letter is to inform you that we are granting your request to restrict your Protected Health Information with a specific person or a specific business that you identified in your Health Information Restriction Form. Your request has been approved.

Your information will not be disclosed to the specified person or entity. We will comply with this request until you tell us to end this restriction unless the information is needed to provide emergency treatment to you.

If you have questions please contact the US TMA, Five Skyline Place, 5111 Leesburg Pike, Falls Church, VA 22041-3206, .

Sincerely

Summary

- You should now be able to:
  - Record a disclosure restriction request
  - Approve or deny the disclosure restriction request
  - Generate an approval or denial letter to be sent to the requester

Authorizations

Objectives

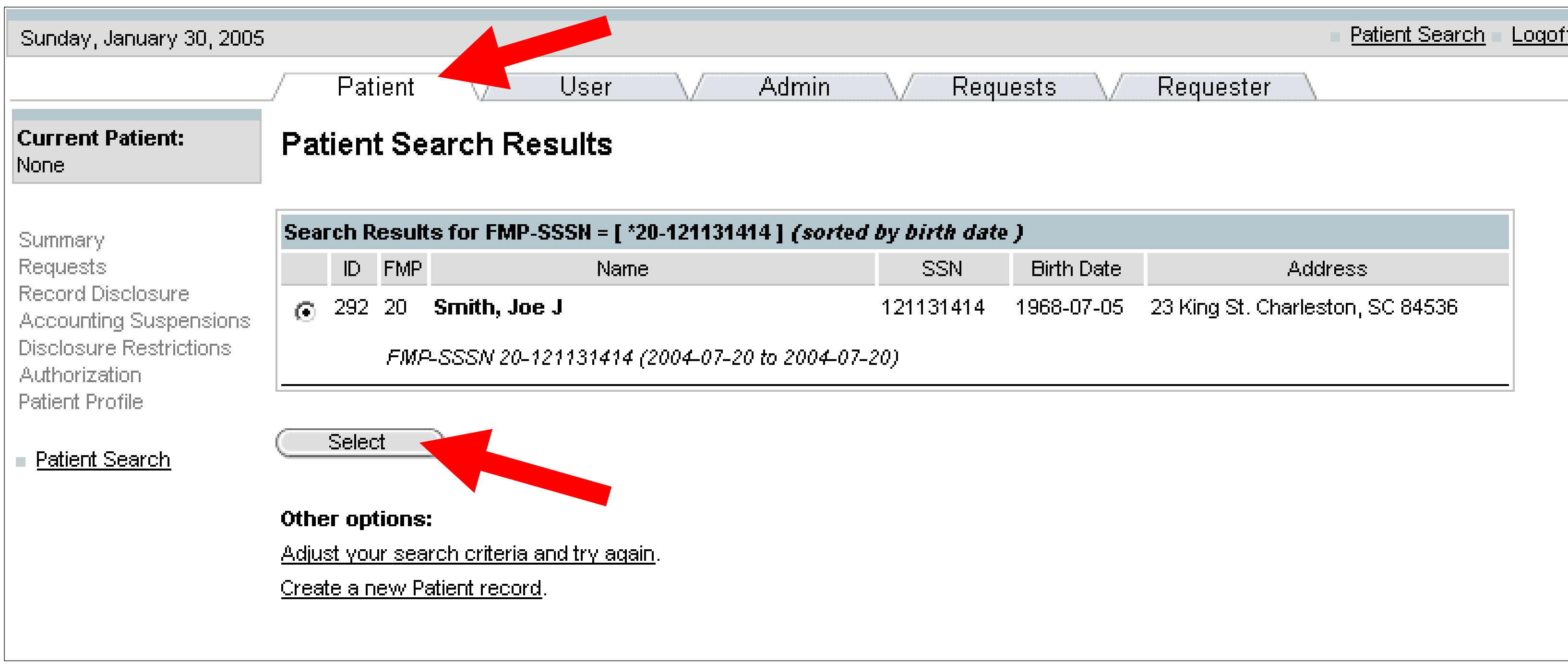
- Upon completion of this lesson, you will be able to:
  - Create an authorization
  - Generate a DD Form 2870
  - Sign an authorization
  - Revoke an authorization

Creating an Authorization (1 of 8)

- The MHS uses the DD Form 2870 (Authorization for Disclosure of Medical or Dental Information)
- Authorizes an individual or organization to disclose a patient’s medical or dental information
- Once an authorization has been created, the DD Form 2870 can be downloaded from the Privacy Office website, or from the DoD Forms website
- Can be generated using PHIMT

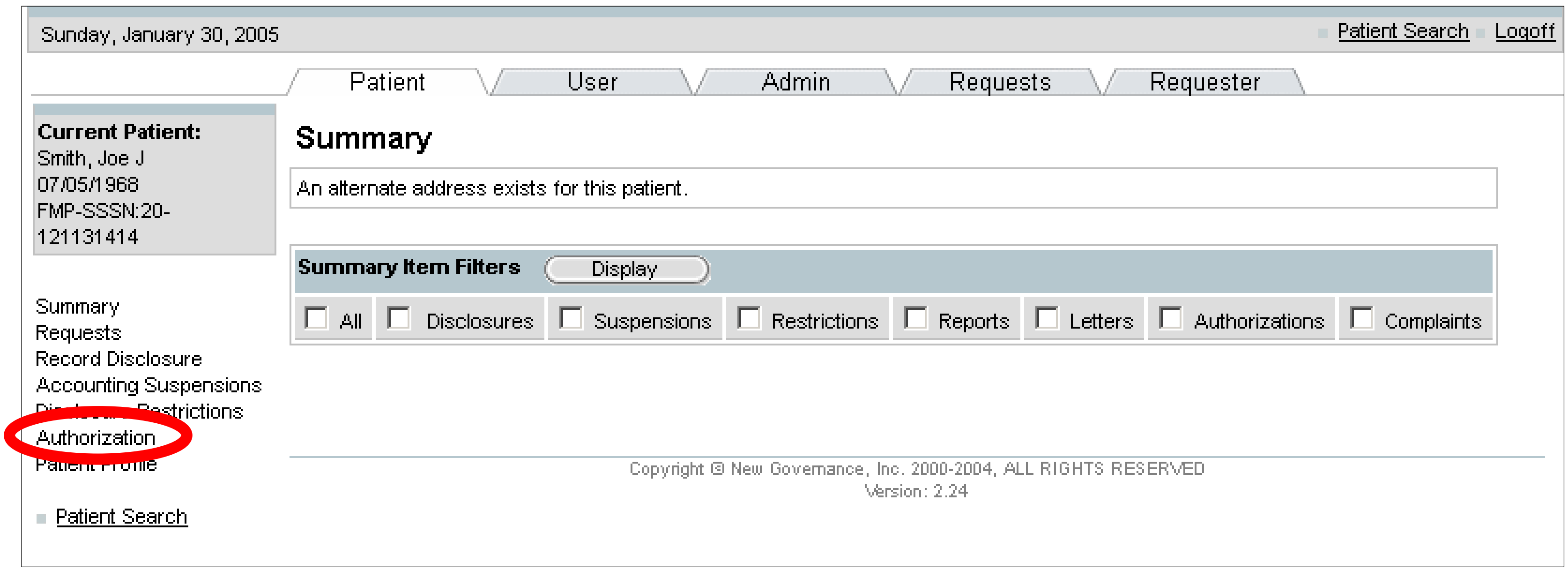
Creating an Authorization (2 of 8)

1. Select the Patient tab
2. Search for and select the patient



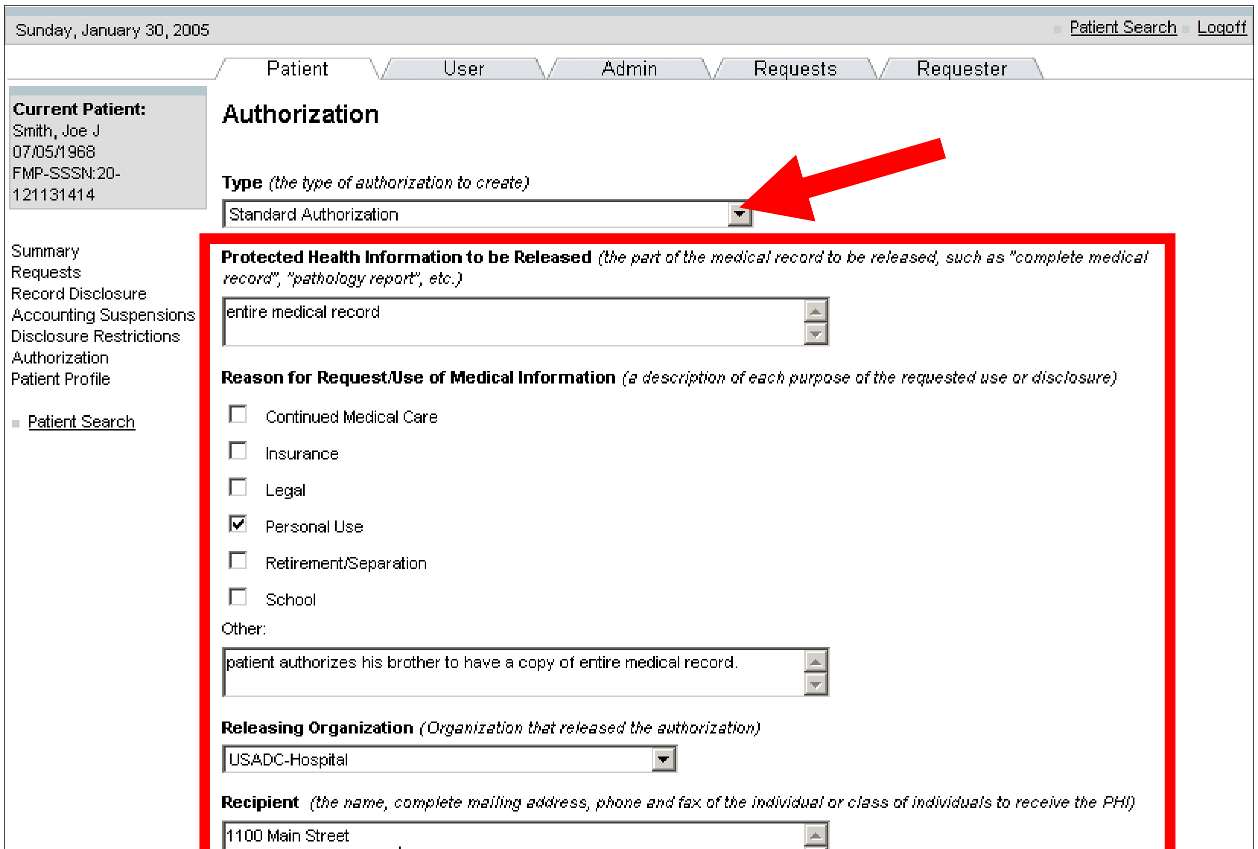
Creating an Authorization (3 of 8)

3. Select the Authorization hyperlink



Creating an Authorization (4 of 8)

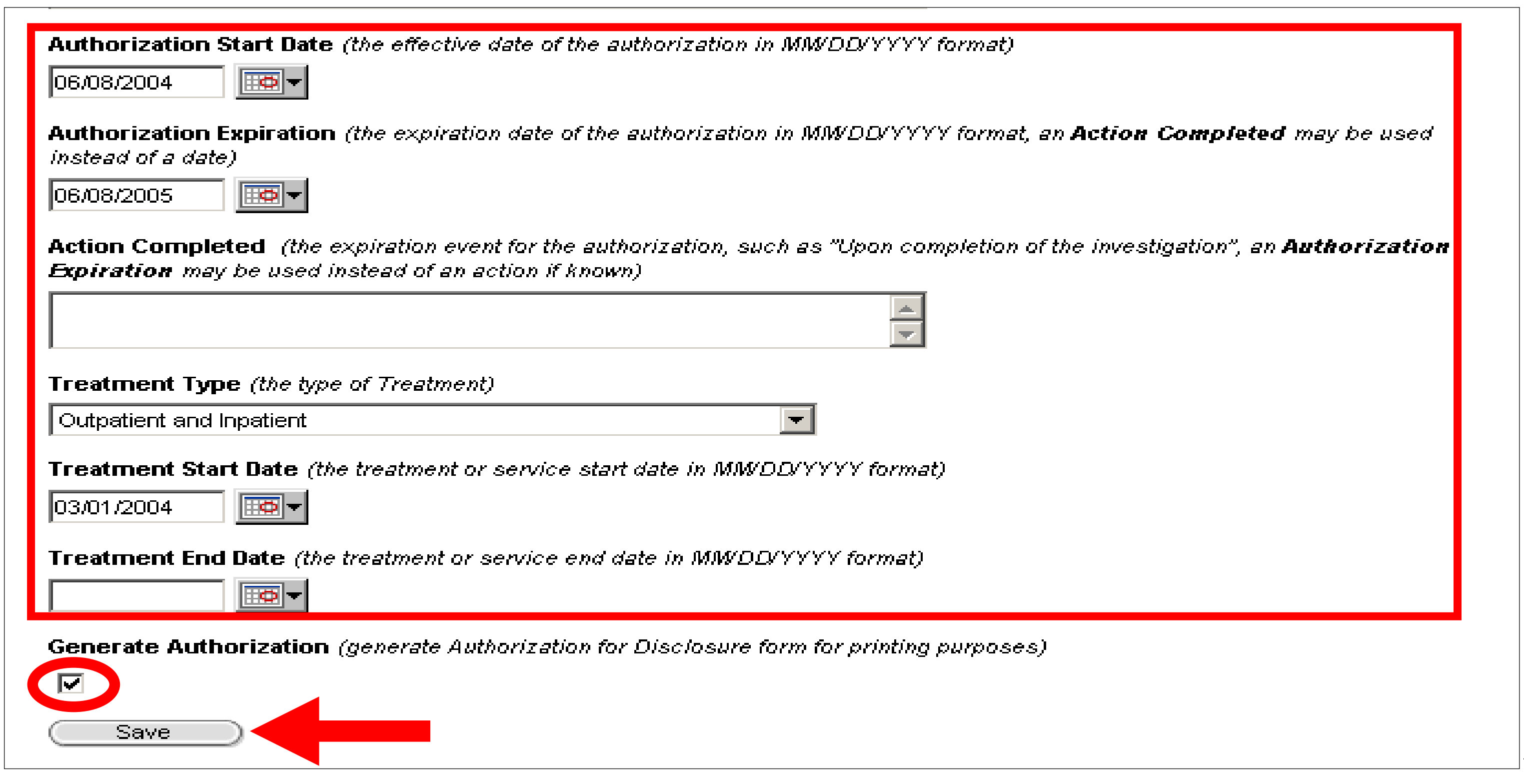
4. Select the Authorization Type from the drop-down box
5. Enter the authorization details: (reason for request, releasing organization, and recipient)



Authorizations

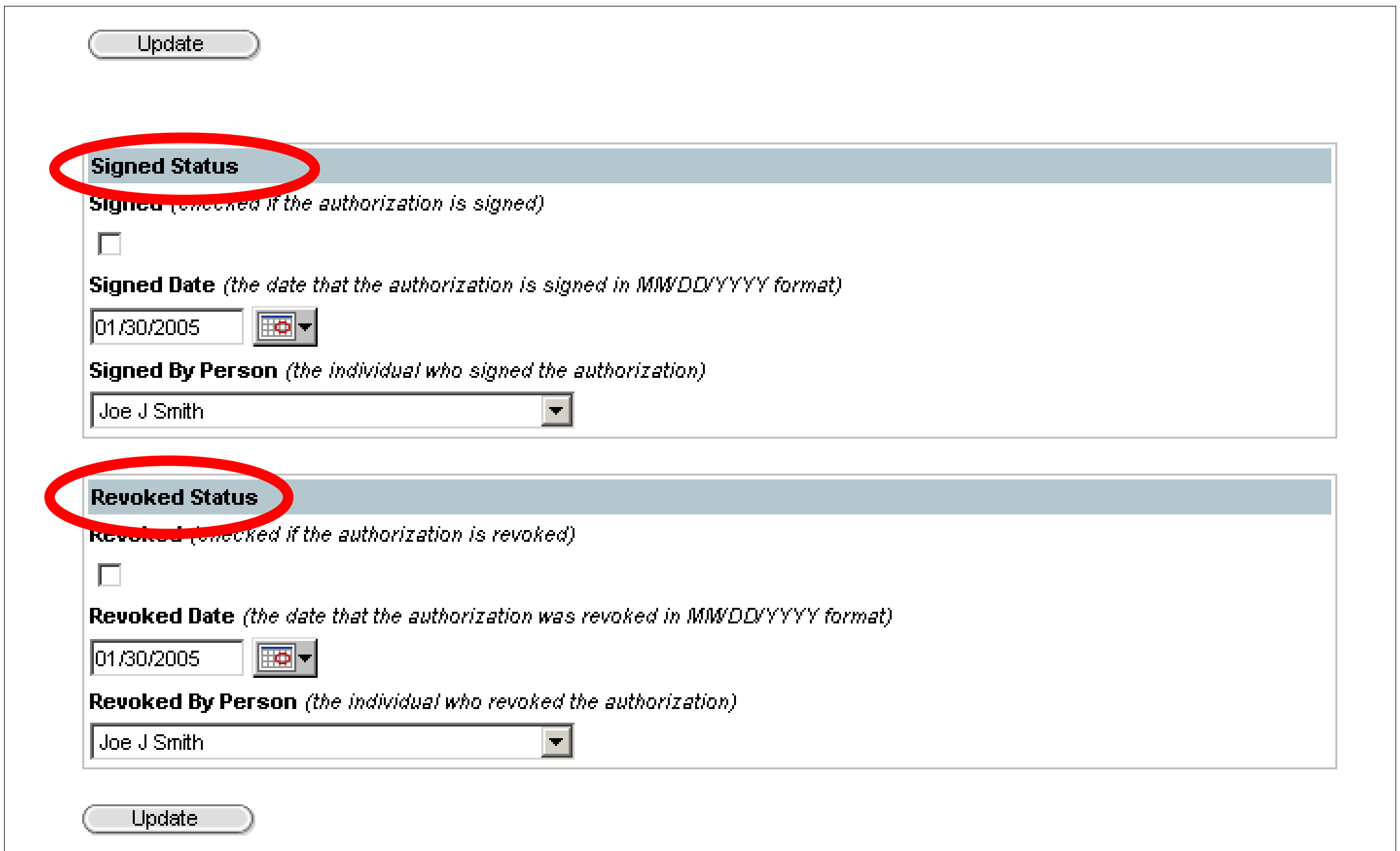
Creating an Authorization (5 of 8)

6. Scroll down the screen and enter: (authorization start and expiration date, treatment type, and treatment start and end date)
7. Place a check in the Generate Authorization checkbox
8. Click on the Save button



Creating an Authorization (6 of 8)

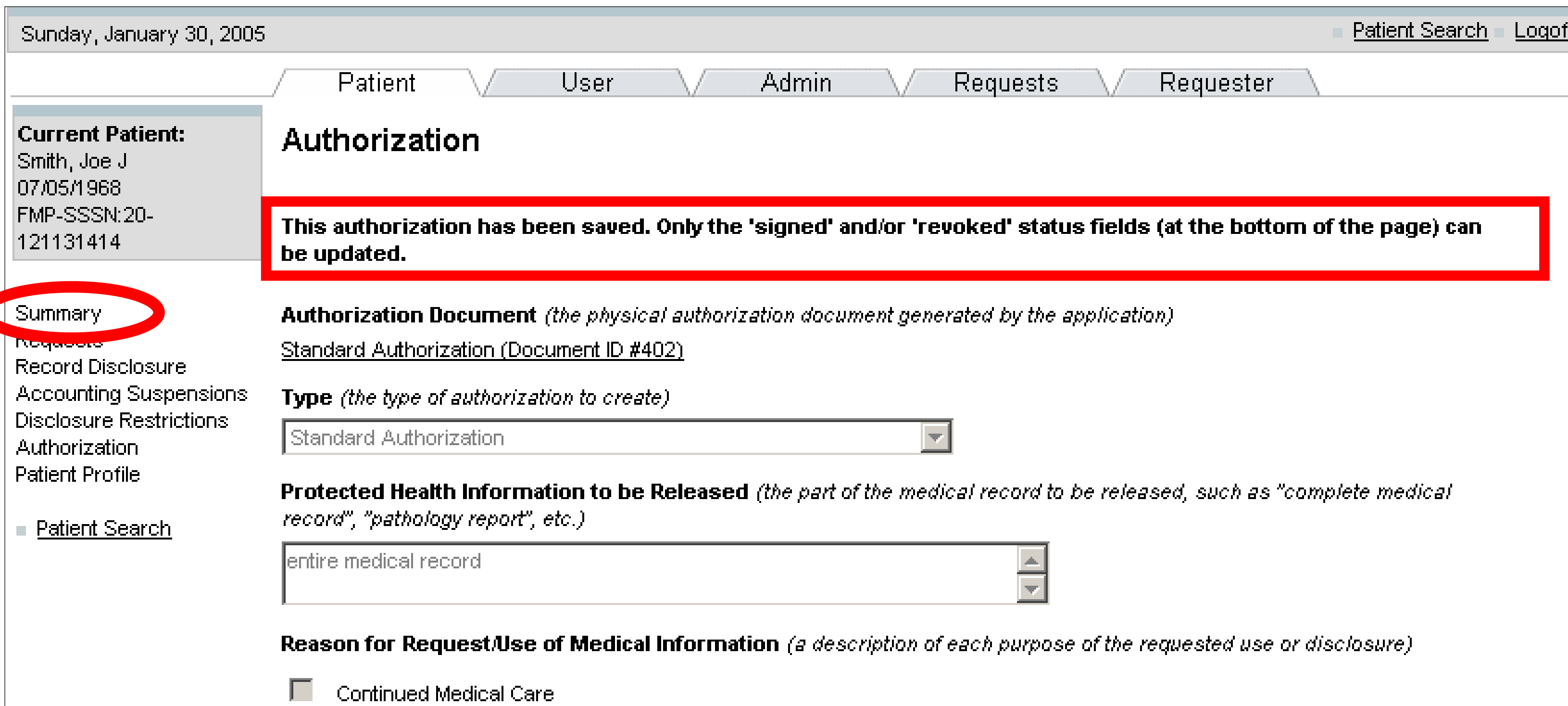
- The Signed Status and Revoked Status boxes on this screen indicate if the DD Form 2870 is signed or revoked



Creating an Authorization (7 of 8)

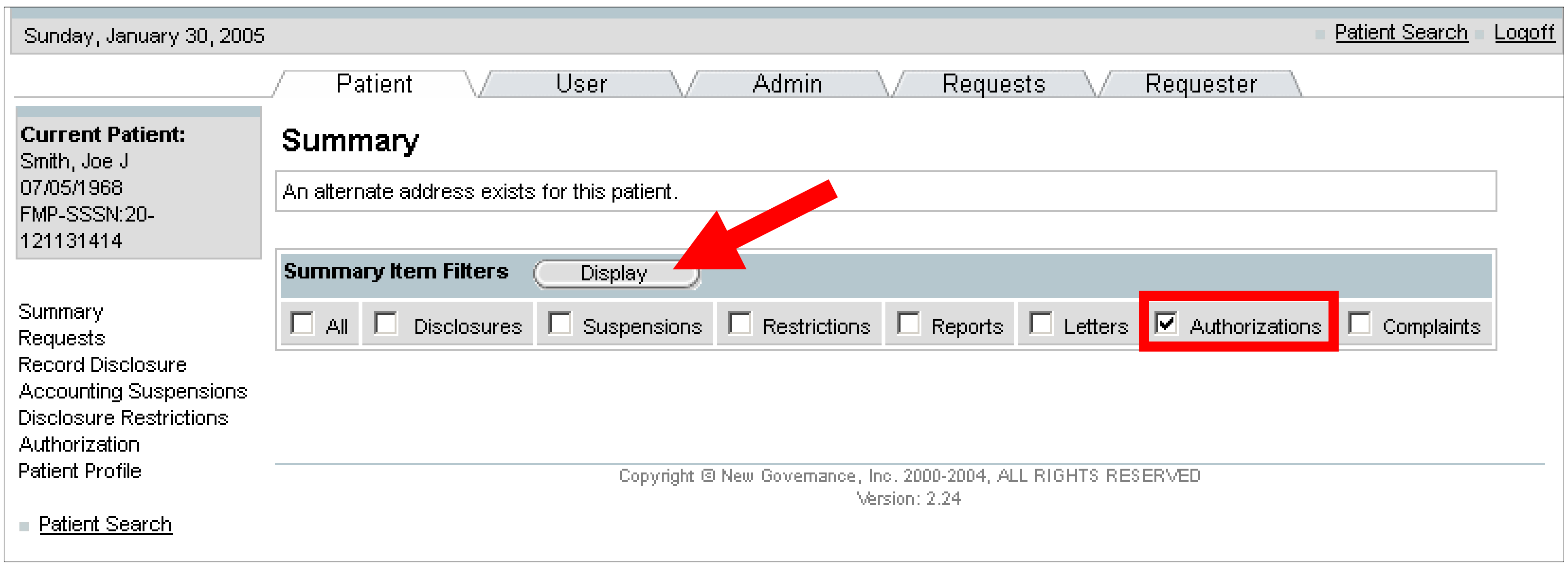
- A note appears at the top of the screen indicating the authorization is saved and that only the “Signed” or “Revoked” status fields may be changed at this point

9. Select the Summary hyperlink



Creating an Authorization (8 of 8)

10. Place a check in the Authorizations checkbox
11. Click on the Display button

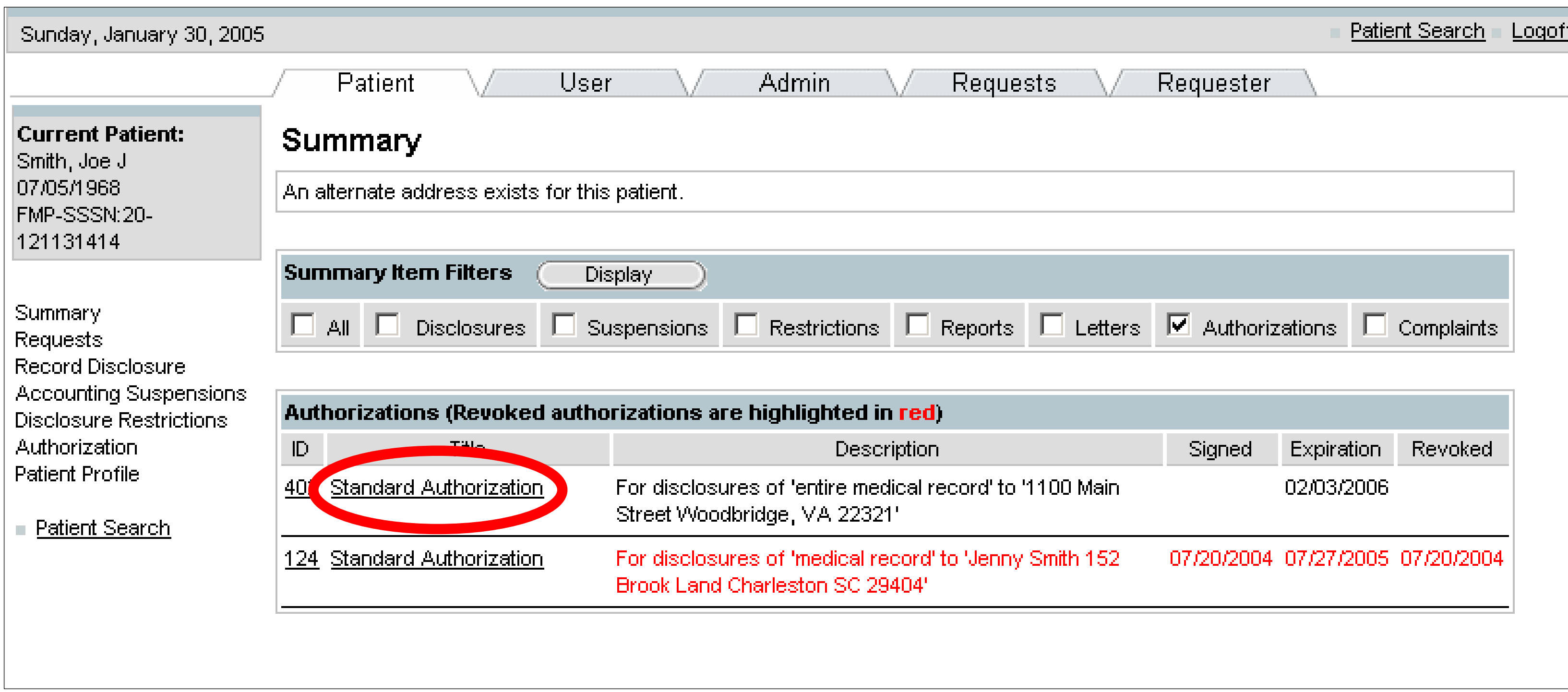


Authorizations

Generate DD Form 2870 (1 of 2)

- The new authorization will appear on the Summary screen

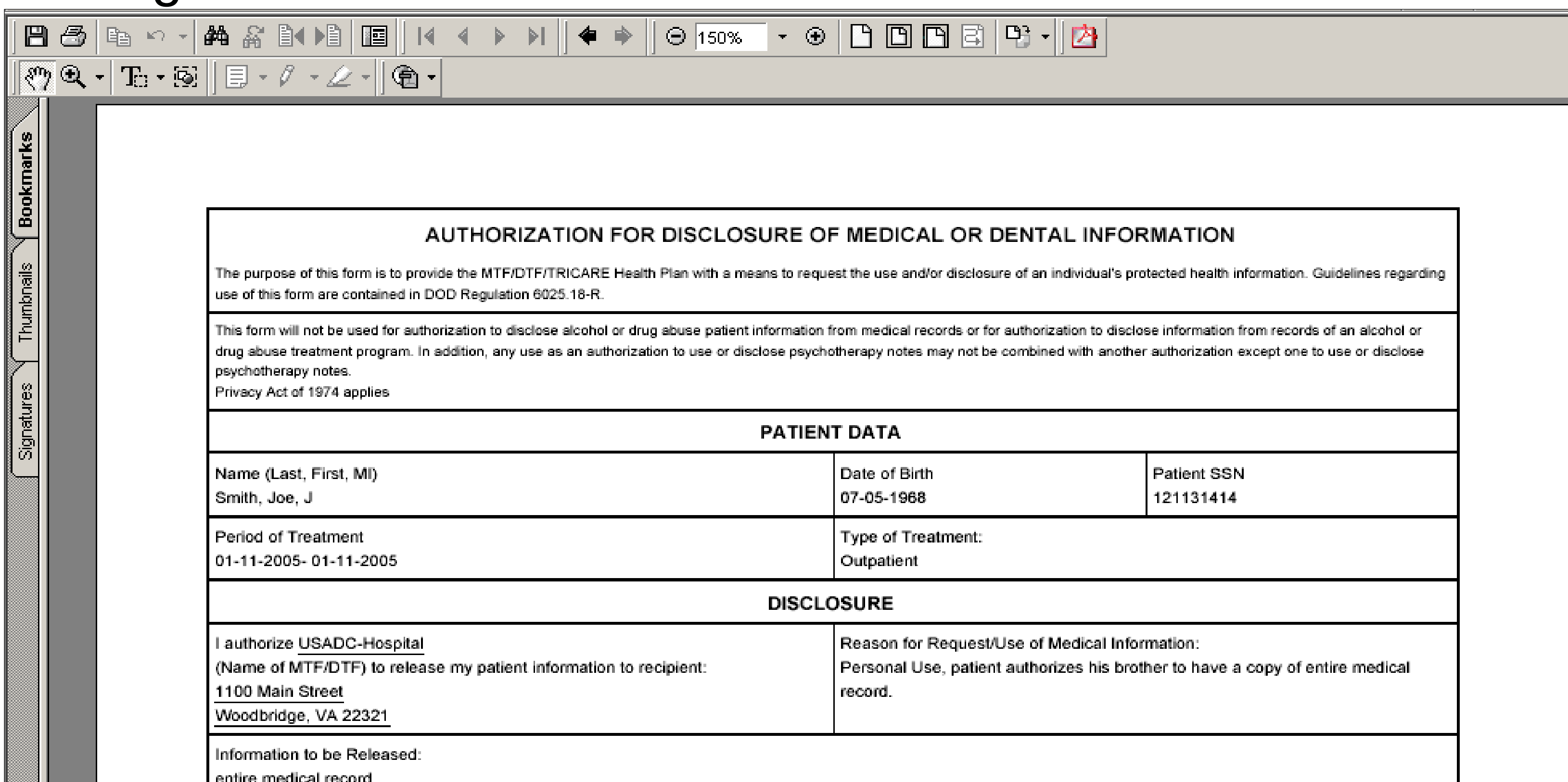
1. Select the authorization title hyperlink to generate DD Form 2870



Generate DD Form 2870 (2 of 2)

- DD Form 2870 in Adobe Acrobat format

2. You may print the form and request the patient's signature



AUTHORIZATION FOR DISCLOSURE OF MEDICAL OR DENTAL INFORMATION

The purpose of this form is to provide the MTF/DTF/TRICARE Health Plan with a means to request the use and/or disclosure of an individual's protected health information. Guidelines regarding use of this form are contained in DOD Regulation 6025.18-R.

This form will not be used for authorization to disclose alcohol or drug abuse patient information from medical records or for authorization to disclose information from records of an alcohol or drug abuse treatment program. In addition, any use as an authorization to use or disclose psychotherapy notes may not be combined with another authorization except one to use or disclose psychotherapy notes.
Privacy Act of 1974 applies

PATIENT DATA

Name (Last, First, MI)	Date of Birth	Patient SSN
Smith, Joe, J	07-05-1968	121131414

Period of Treatment	Type of Treatment:
01-11-2005- 01-11-2005	Outpatient

DISCLOSURE

I authorize USADC-Hospital (Name of MTF/DTF) to release my patient information to recipient: 1100 Main Street Woodbridge, VA 22321	Reason for Request/Use of Medical Information: Personal Use, patient authorizes his brother to have a copy of entire medical record.

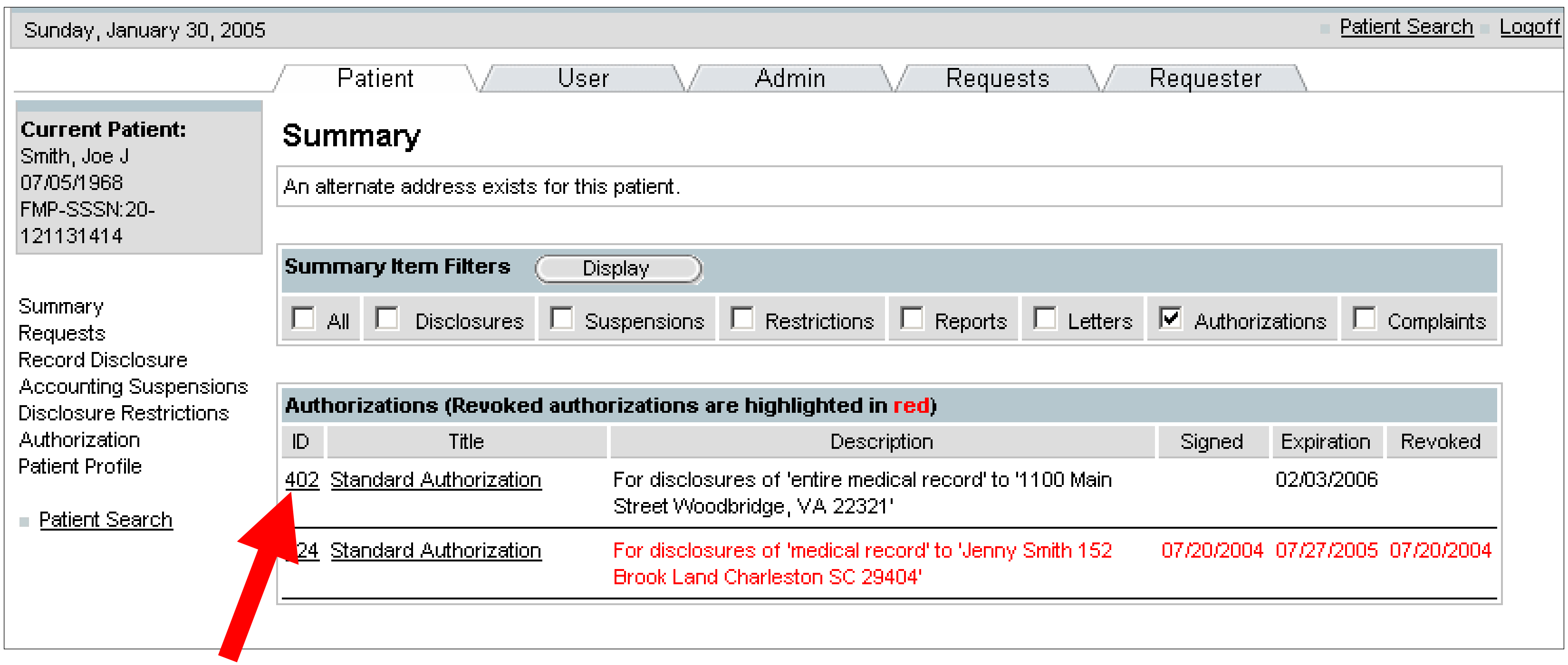
Information to be Released:
entire medical record

Signing an Authorization (1 of 5)

- Once an authorization has been entered, it needs to be signed by the patient for validation
- After the authorization is signed by the patient, a user has the ability to document the signature within the PHIMT

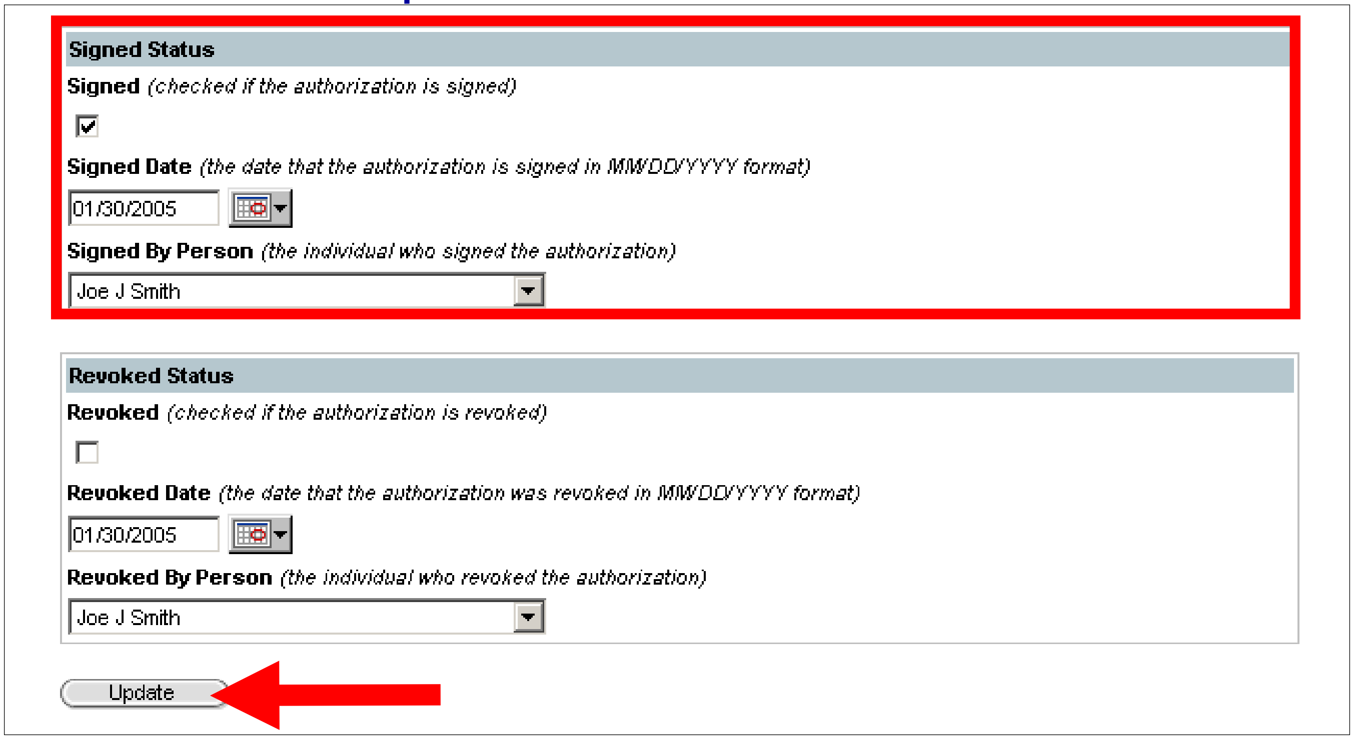
Signing an Authorization (2 of 5)

1. Select the authorization ID hyperlink to return to the detailed authorization record



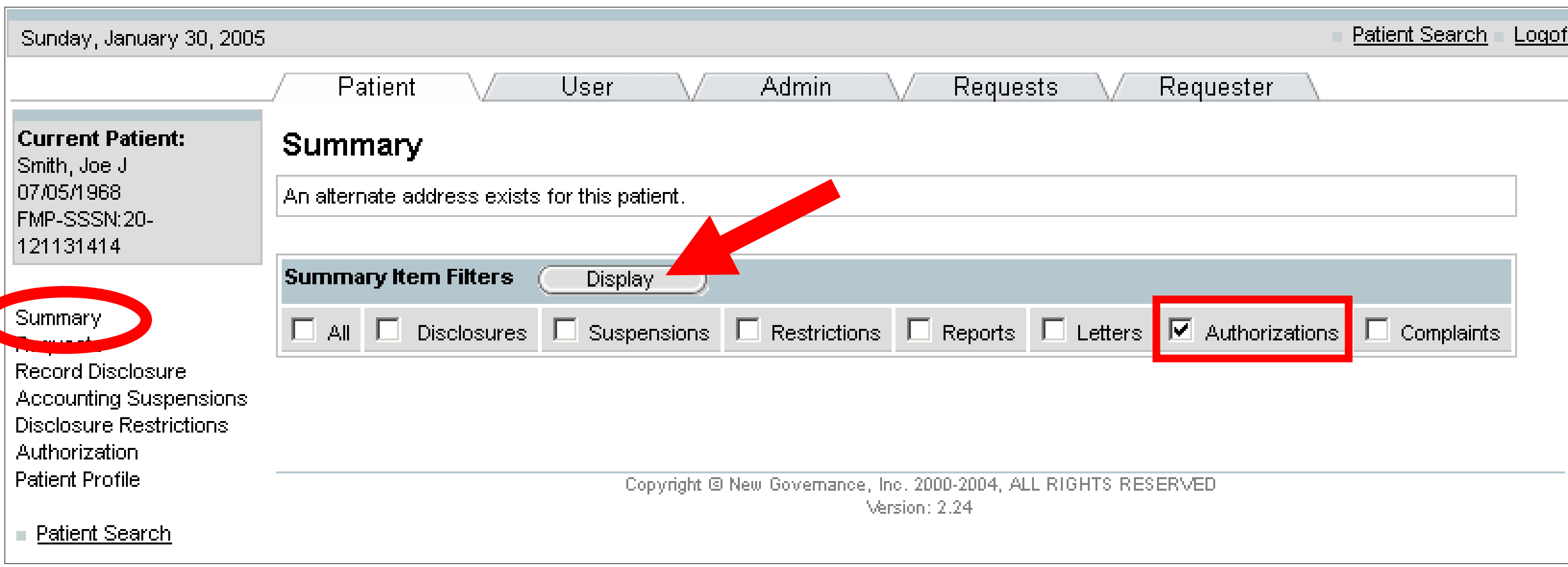
Signing an Authorization (3 of 5)

2. Scroll to the bottom of the page to the Signed Status box
3. Place a check in the Signed Status checkbox
4. Select the date and the authorizing person's identity from the drop-down box
5. Click on the Update button



Signing an Authorization (4 of 5)

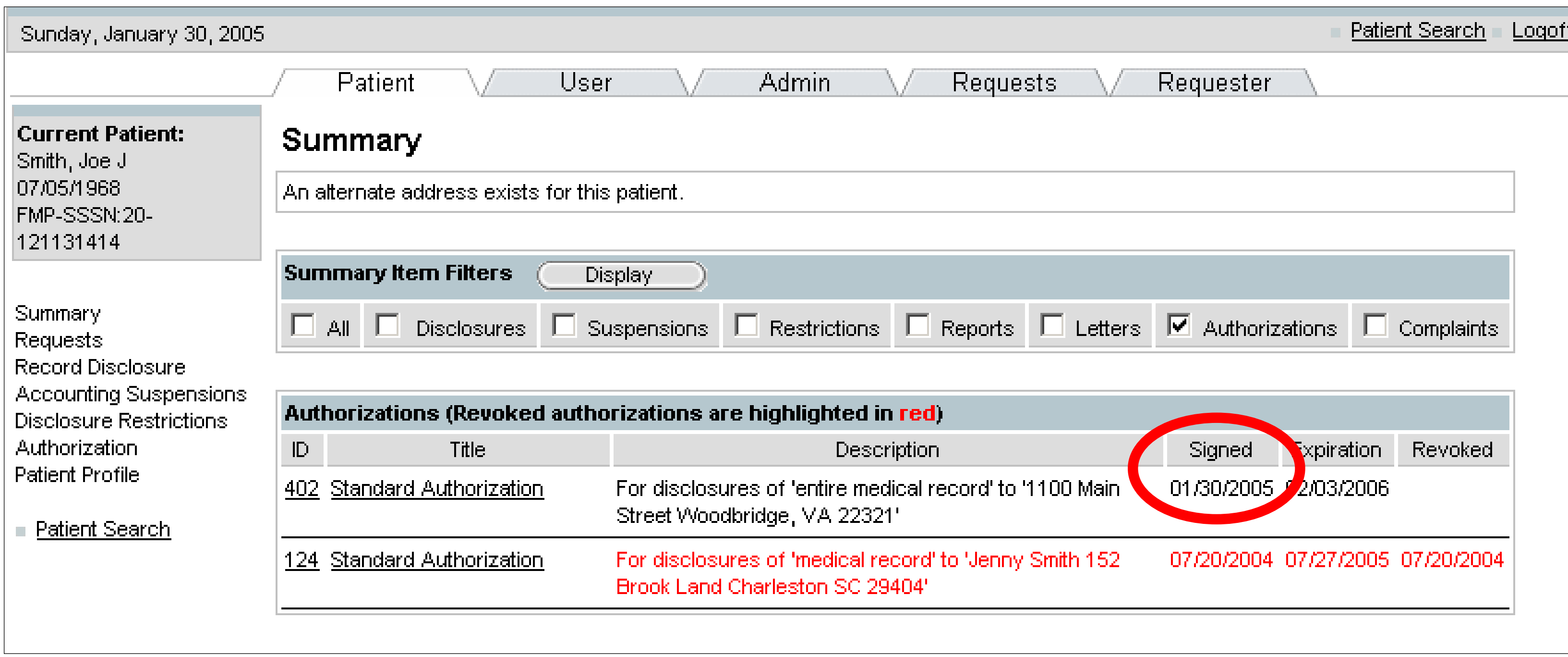
6. Select the Summary hyperlink
7. Place a check in the Authorizations checkbox
8. Click on the Display button



Authorizations

Signing an Authorization (5 of 5)

- You will now see that the authorization indicates that it has been signed

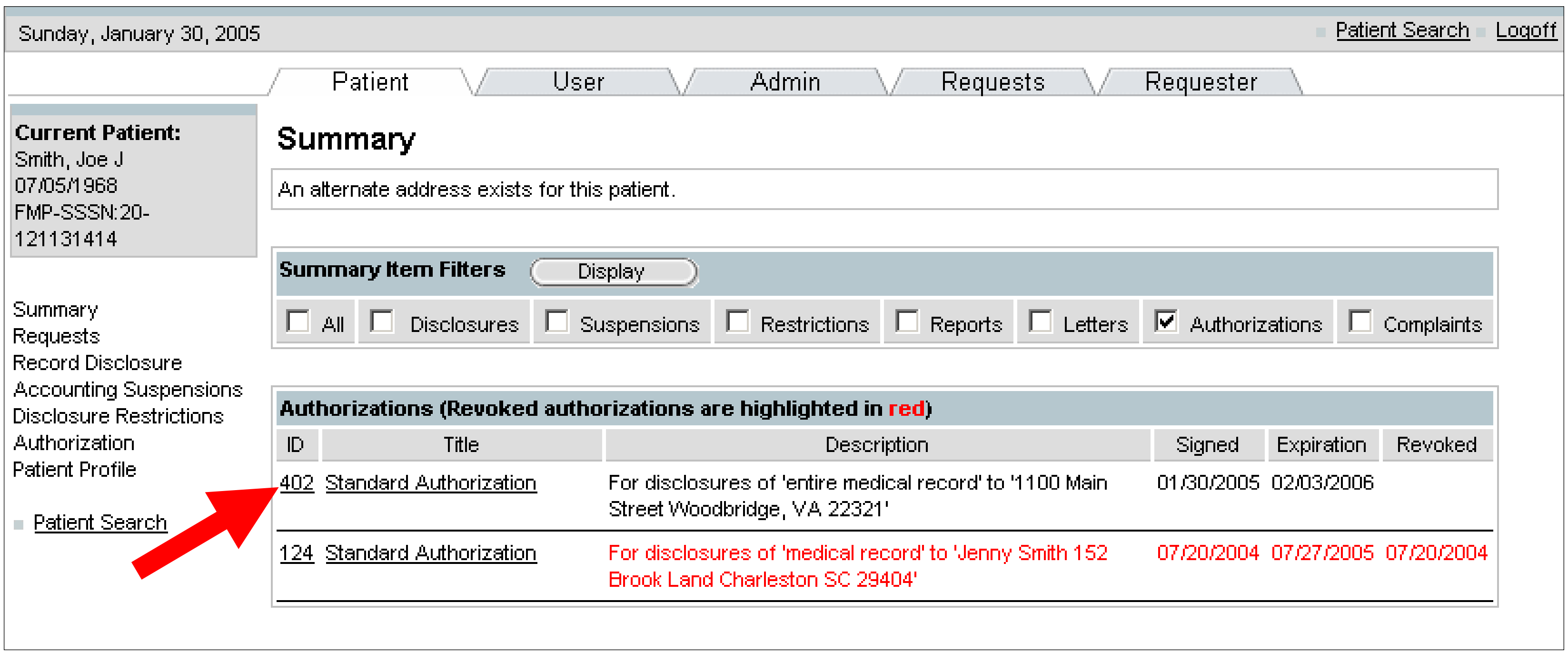


Revoking an Authorization (1 of 5)

- DoD 6025.18-R, Section C5.2.5
- Privacy Specialists can revoke an authorization when instructed by a patient in writing
  - Except if:
    - The covered entity has taken action in reliance thereon
    - Insurance coverage

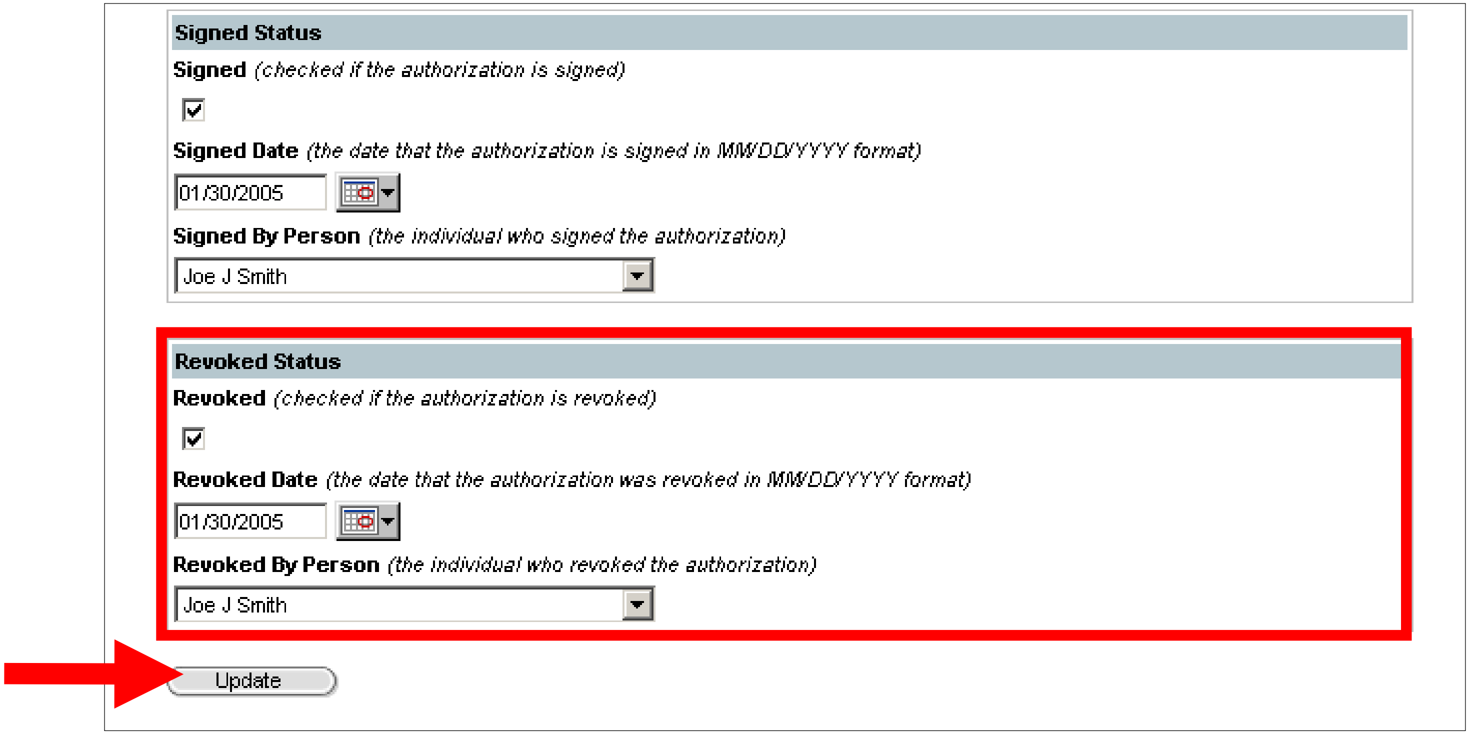
Revoking an Authorization (2 of 5)

1. Select the authorization ID hyperlink



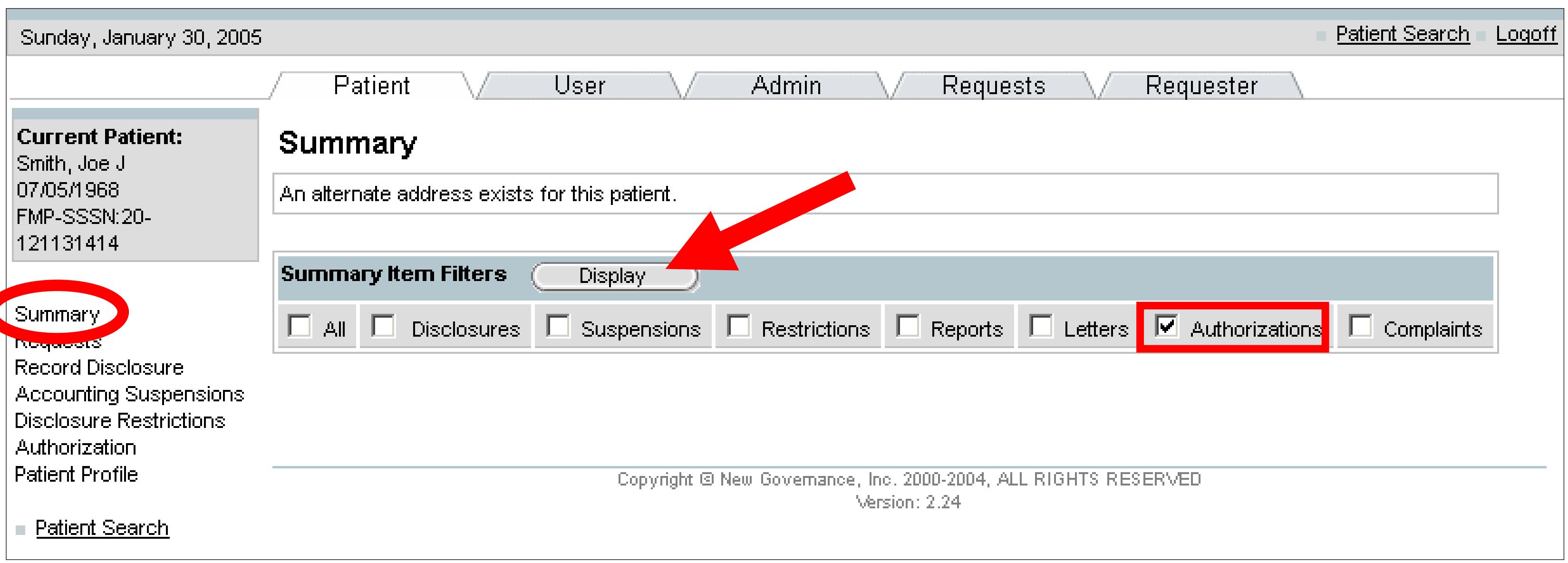
Revoking an Authorization (3 of 5)

2. Scroll to the bottom of the screen to the Revoked Status box
3. Place a check in the Revoked check box
4. Select the date and the revoking person's identity in the drop-down box
5. Click on the Update button



Revoking an Authorization (4 of 5)

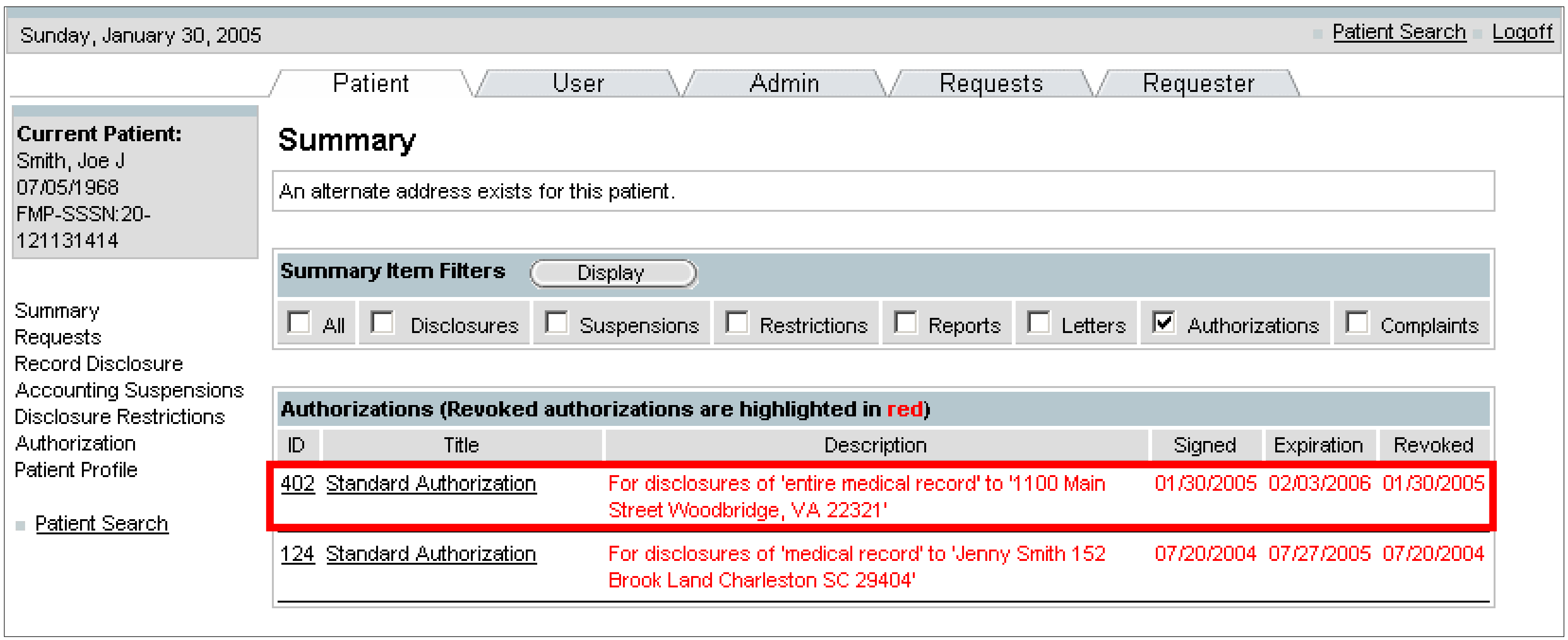
6. Select the Summary hyperlink to view the authorization
7. Place a check in the Authorizations checkbox
8. Click on the Display button



Authorizations

Revoking an Authorization (5 of 5)

- The revoked authorization is highlighted in red



Summary

- You should now be able to:
  - Create an authorization
  - Generate a DD Form 2870
  - Sign an authorization
  - Revoke an authorization

Administrative Summary

Objectives

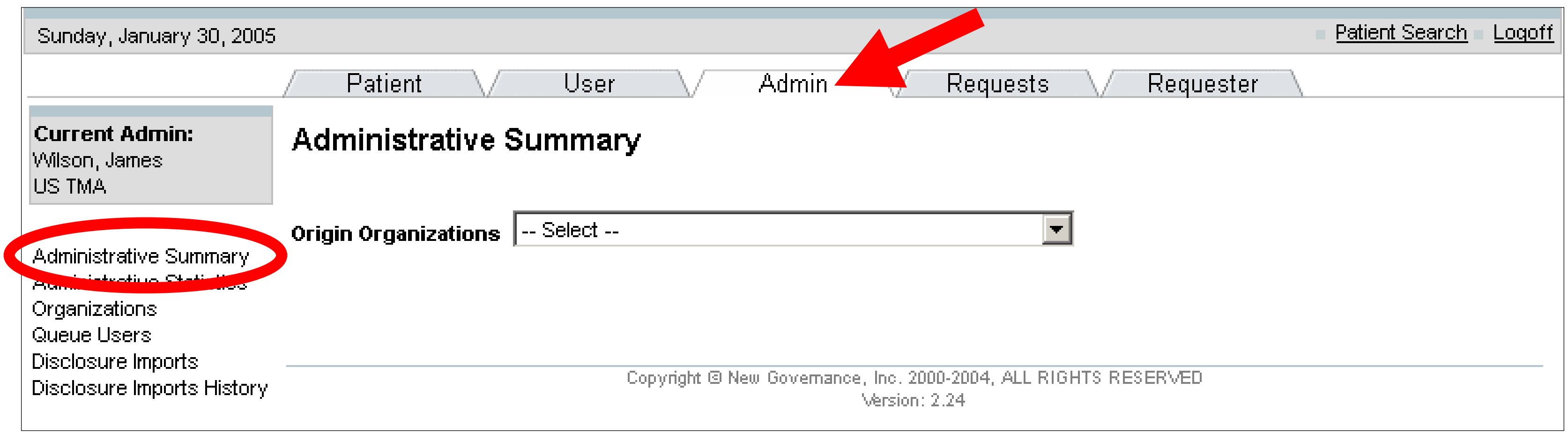
- Upon completion of this lesson, you will be able to:
  - View administrative summary reports

Administrative Summary Reports (1 of 4)

- Administrative summaries provide a visual representation by organization of:
  - Disclosures over a 12 month period
  - All requests by type
  - All requests over a 12 month period
  - Top recipients of disclosures
  - Top requesters for all requests
- Performed by Privacy Specialists and User Admins

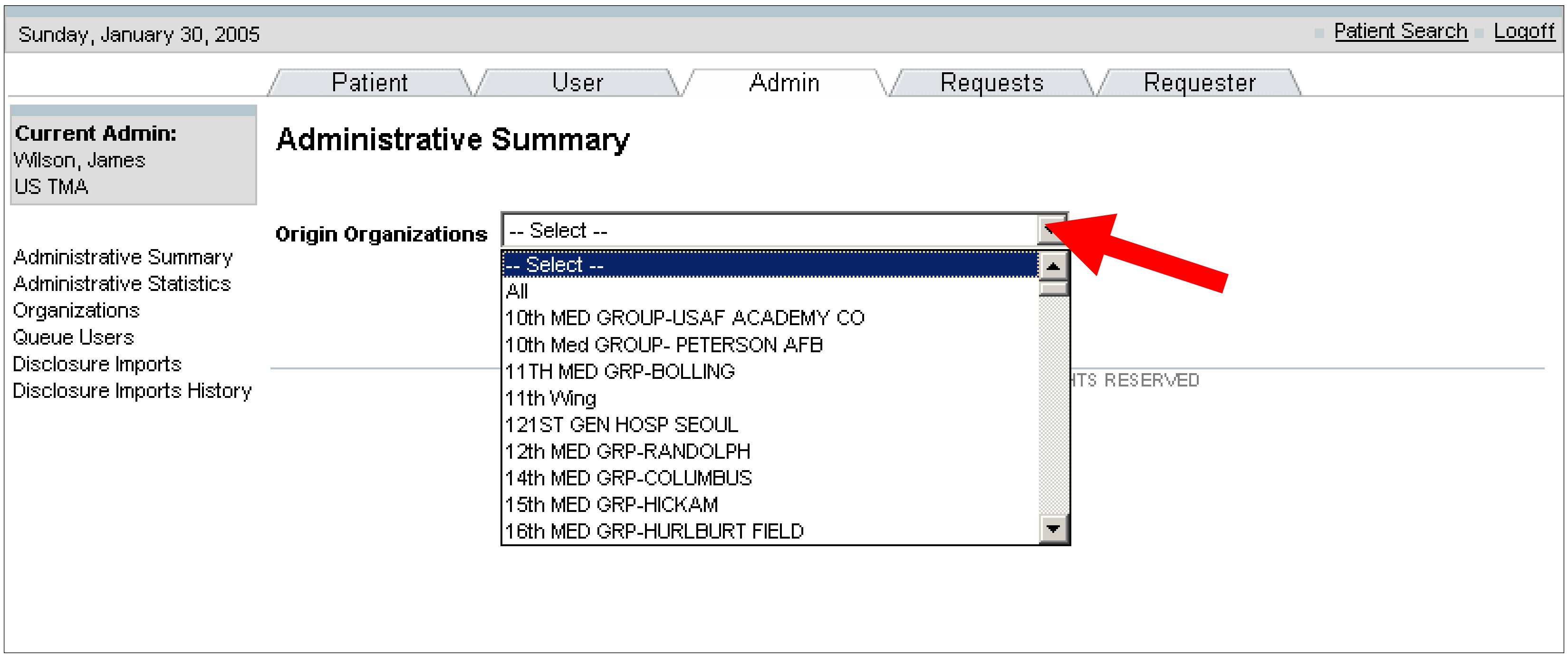
Creating Administrative Summary Reports (2 of 4)

1. Select the Admin Tab
2. Select the Administrative Summary hyperlink



Creating Administrative Summary Reports (3 of 4)

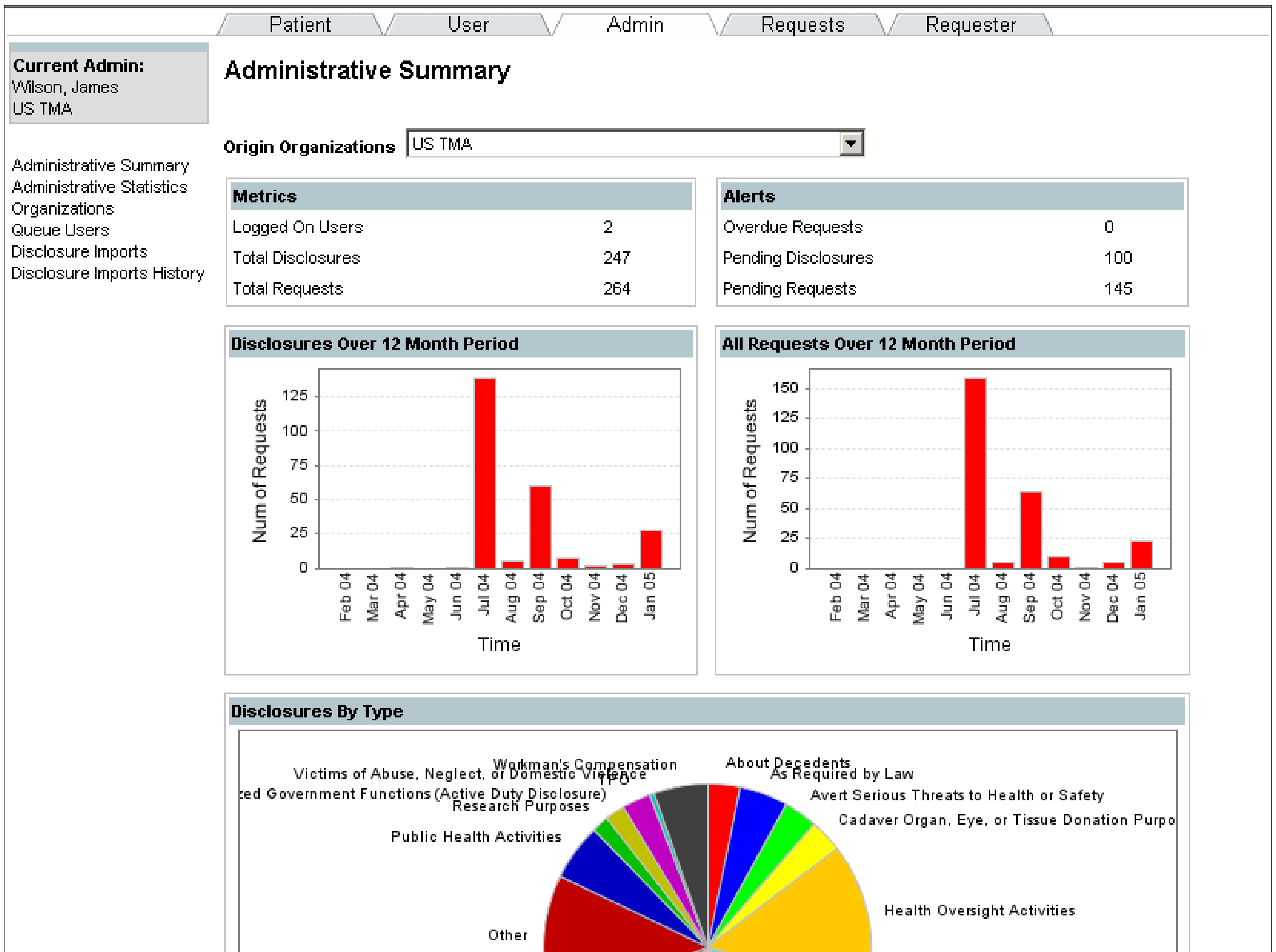
3. Select your Organization from the drop-down box



Administrative Summary

Creating Administrative Summary Reports (4 of 4)

- The Administrative Summary reports will display



Summary

- You should now be able to:
  - View administrative summary reports

PHIMT

Presentation Summary

- You should now be able to:
  - Describe the PHIMT application
  - Identify the user roles and permissions
  - Perform the functions of the User Admin, Privacy Specialist, and Regular User within the PHIMT

Resources

- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003

- www.tricare.osd.mil/tmaprivacy/HIPAA.cfm

- privacymail@tma.osd.mil for subject matter questions

- hipaasupport@tma.osd.mil for tool related questions

- http://www.tricare.osd.mil/tmaprivacy/Mailing-List.cfm to subscribe to the TMA Privacy Office E-News

- Service HIPAA Privacy representatives

HEALTH AFFAIRS

TRICARE Management Activity

Please fill out your critique

Thanks!